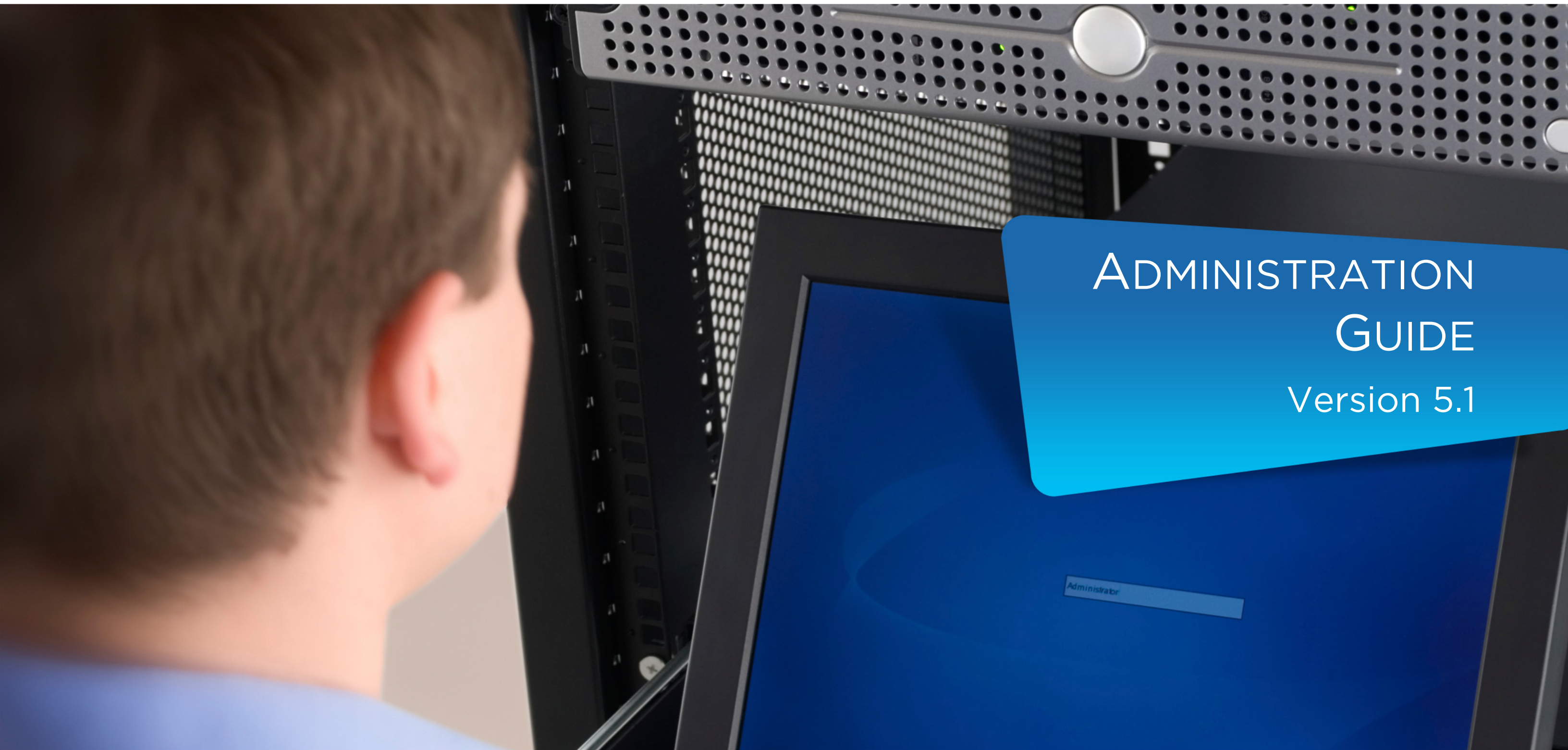
VIRCOM
email security matters

modusGate™



Administration Guide

Version 5.1

Vircom copyright statement

The contents of this manual are for informational use only and are subject to change without notice. Neither Vircom nor anyone else who has been involved in the creation or production of this manual assumes any responsibility or liability for any errors or inaccuracies that may occur in this manual, nor for any loss of anticipated profit or benefits, resulting from the use of this manual.

This manual is protected by copyright laws and international treaties. Your right to copy this manual is limited by copyright law and the terms of your software license agreement. As the software licensee, you may make a reasonable number of copies or printouts, provided they are for your own use. Making unauthorized copies, adaptations, compilations or derivative works for any type of distribution is prohibited and constitutes a punishable violation of the law.

Any references to names of actual companies, products, people and/or data used in screenshots are fictitious and are in no way intended to represent any real individual, company, product, event and/or data unless otherwise noted.

directQuarantine™, modus™, and modusGate™ are all trademarks of Vircom Inc. Windows®, Windows® 2000 Server, Windows® Server 2000/2003/2008, IIS, Internet Information Server, Windows® Exchange Server, Active Directory, Windows® SQL and Microsoft® Outlook are either registered trademarks or trademarks of Microsoft® Corporation in the United States and/or other countries. All other products or services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations.

modusGate is based on the Professional Internet Mail Services product licensed from the University of Edinburgh.

Certain algorithms used in parts of this software are derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm.

Vircom Inc., 460 St. Catherine W, Suite 600, Montreal, QC, Canada, H3B 1A7

For more information, contact Customer Support at +1 514.845.8474, Toll-free at 1.888.484.7266, Sales at +1.514.845.1666, Ext. 1 or visit our website at www.vircom.com

Section 1

Introduction

About this manual

Intended audience

This document is written for administrators installing and configuring the modusGate™ application in a Windows® Server environment. It is assumed that the reader is familiar with:

- Microsoft® Windows® operating system.
- Vircom concepts.
- Microsoft SQL® servers.

Purpose and scope

This document is designed to provide you with instructions to install and configure modusGate Server and its web applications.

Formatting conventions

The following formatting conventions are used in this document.

The text attribute	Is used for
Bold	New terms defined for the first time.
Hyperlink	Clickable links to the referenced topic.
Italic	Titles used in cross-references and other Vircom documents.
Franklin Gothic Book font	All output, text labels from a graphic user interface, and for anything you would type into the user interface.
<Key>	Keyboard keys, like <Ctrl>, <Alt>, <Shift>, <Del>, etc.

Product names

The following product names are used in this guide.

The term	Means
modusGate L	Email relay gateway with network-level security only (does not include anti-virus or anti-spam protection).
modusGate AS	Email relay gateway with anti-spam protection, including phishing and attachment blocking, custom sieve scripts and a full year of SCA spam engine updates.
modusGate AV	Email relay gateway with anti-virus protection. Comes with a full year of virus protection from McAfee or Norman Data Defense.
modusGate ASV	Email relay with both anti-spam protection and anti-virus protection, including spam, phishing, virus and forbidden attachment blocking. Comes with a full year of virus protection from McAfee or Norman Data Defense.

Help and support

Contact Vircom Technical Support team

If you have specific questions concerning the use of one of our products, please contact the Technical Support team at Vircom Inc.

Web:	http://www.vircom.com
E-mail:	support@vircom.com
Phone:	1.514.845.8474
Toll free:	1.888.484.7266
Fax:	1.514.845.6922
Working hours:	Regular business hours 7:30 AM to 6:00 PM EST, Monday-Friday

Knowledge Base

For additional information, please see Vircom’s Knowledge Base at:

http://kb.vircom.com/kbase

The Knowledge base contains the most recent versions of all modusGate documents, bulletins, fixes and patches, known issues and configuration how-to’s.

Related documents

The documentation set for modusGate includes the following:

WebQuarantine User Guide

directQuarantine Administration Guide

They can be found in the modusGate Documents directory: ...\Vircom\modusGate\Documents, and in the Knowledge Base.

Section 2

Getting Started

Configuration requirements

modusGate integration

modusGate is a comprehensive email security gateway server that is compatible with Windows® Server 2003, Windows Server 2008, 2008 R2 and Virtual Machines (VM). It integrates with Microsoft® Exchange®, Lotus® Domino® and any standard SMTP server.

Because modusGate was designed primarily to work with Microsoft Exchange, this section of the document will focus on its configuration with Exchange and Active Directory.

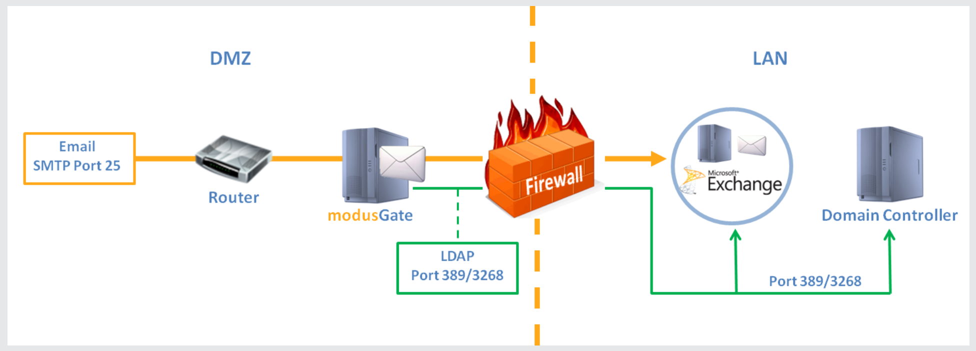
NOTE For deployment with Lotus Domino and other SMTP servers, please see our Knowledge Base for details:

http://kbase.vircom.com/kbase/default.asp?id=1265&Lang=1&SID=

Deployment scenarios

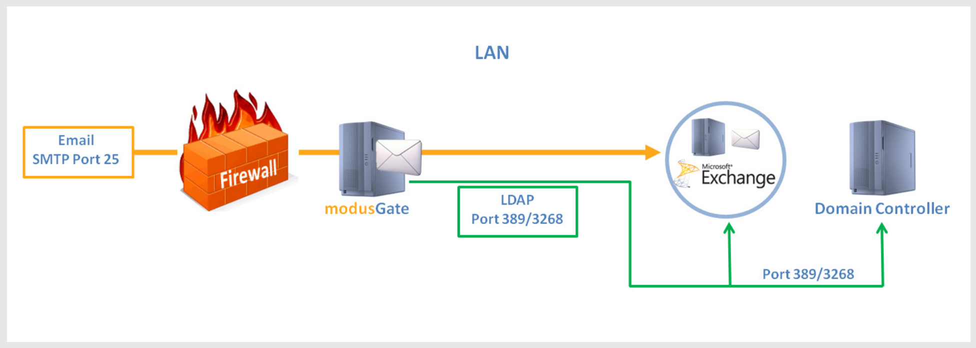
Scenario 1: modusGate in the DMZ

With this method, modusGate resides in the DMZ while the Exchange Server and other network resources are protected behind a firewall.



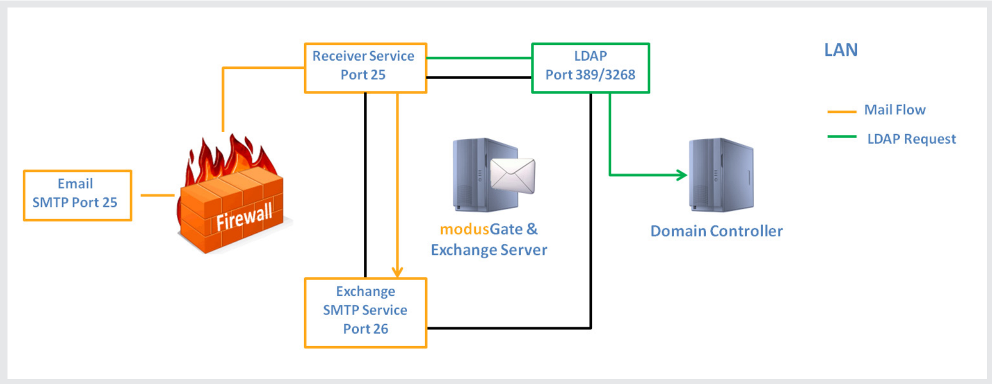
Scenario 2: modusGate on the same subnet as Exchange

Here, the firewall provides Network Address Translation (NAT) or simple port filtering. After modusGate is installed and configured, change the NAT rule to route mail to modusGate instead of directly to Exchange.



Scenario 3: modusGate installed on the Exchange Server

Note that this setup is not recommended, but can suffice if mail traffic is quite low. In this option, modusGate must be configured to receive mail on Port 25, while Exchange must be modified to use a different port, e.g. 2525.



System requirements

The following are the recommended minimum system requirements for modusGate Server:

Requirement	Description
Windows Server OS	Windows Server 2003, 2008, 2008 R2 (64-bit) with the most recent Service Pack. Virtual Machines (VM) are also supported. NOTE modusGate Server cannot be installed on a Windows Web Edition Server (any version).
CPU	2.13 GHz Intel® Pentium® IV processor.
Disk	40 GB (or higher), 7200 RPM hard drive (mirrored is recommended) NTFS with Indexing disabled.
Memory	1024 MB RAM.
MDAC	Microsoft Data Access Component 2.8 SP1 or higher.
DNS Server	Must be accessible by modusGate.
IIS	Internet Information Server, version 6.0 or higher. May be installed on the modusGate server or on a separate computer.
.NET 3.5 SP1 and 4.0 Extended	.NET Framework versions 3.5 SP1 and 4.0 Extended are both required.

Requirement	Description
SQL Server	Microsoft SQL Server 2000, 2008, 2008R2 or SQL Server 2005 Express Edition. It is recommended that SQL be installed on a separate, standalone computer.
IE 6 or above	Required for WebMonitor and WebAdmin access.
Adobe® Acrobat Reader	Version 7 or higher, required to read the administration guides.

Database requirements

modusGate requires databases for several of its features. If you do not have a database server installed, the modusGate installation process includes Microsoft SQL Server 2005 Express with advanced services. Note that Full Text Indexing is required for some features.

Firewall configuration

If you plan to use a firewall, Vircom recommends that you do not use Windows Firewall as it can cause problems with internal communication required by modusGate. Instead, use a hardware firewall to protect your network from unauthorized external access.

Exchange / Active Directory configuration

Before you begin the modusGate installation, verify the following settings on your Exchange / Active Directory server to ensure proper communication with modusGate:

Step	Description
1	If using Exchange 2007 or 2010, check whether the Hub Transport or Edge Transport server role is installed. If either role exists, you must change the following message throttling settings under **Set-ReceiveConnector:** • **MaxInboundConnectionPercentagePerSource:** Change the value to 20% • **MaxInboundConnectionPerSource:** Change the value to 1000 NOTE For complete details, see the following Microsoft KB articles: **Exchange 2007:** http://technet.microsoft.com/en-us/library/bb232205(EXCHG.80).aspx **Exchange 2010:** http://technet.microsoft.com/en-us/library/bb232205.aspx#ReceiveConn
2	If you are using Exchange 2007 or 2010, it must be configured to accept mail relay from modusGate. Please use this Microsoft Technet article for configuration instructions: http://exchangepedia.com/2007/01/exchange-server-2007-how-to-allow-relaying.html
3	Ensure that you have an account with Read permissions on the Active Directory/Global Catalog; this account and its password will be required when configuring modusGate. You may use your Administrator (SA) account, but it is recommended to create a new account for this purpose. Follow the steps below to create a new account:
4	Log into the Domain Controller Server and go to Start > Programs > Administrative Tools > Active Directory Users and Computers.
5	Expand your domain name, right-click Users and select New > User.
6	Enter mgate in First name, copy it to User logon name and click Next.
7	Configure the Password, uncheck User must change password at next logon, check Password never expires, and click Next through the remaining screens to finish creating the user.
8	Click on View > Advanced Features.
9	Select Security, click on Add and enter mgate.
10	Under the Allow column, check Read and click Apply.

Section 3

Install modusGate

Before you begin

Preinstallation checklist

Before beginning the installation, please review the following checklist of configuration requirements. These will ensure that modusGate is fully functional after completing the install:

Item	Action
1	The server must be configured with a static IP and at least 1 DNS server address. Go to Local Area Connection settings > Properties > Internet Protocol (TCP/IP) > Properties
2	The domain name must be specified in the Network Identification properties: Go to My Computer >Properties > Network Identification > Properties Confirm that the computer name appears in the Computer name field. Click on More > Primary DNS suffix for this computer and enter your domain name. The server must be rebooted after this change. NOTE If this information is missing, the modusGate installer will automatically prompt you to enter it at the end of the install process and launch a server reboot.
3	IIS 6.0 or above is already installed.
4	Both .NET Framework versions 3.5 SP1 and 4.0 Extended are installed.
5	Microsoft's built-in SMTP service is either disabled or set to manual (required to prevent conflicts on port 25). Go to Administrative Tools > Services and set Simplified Mail Transport Services to Stop.
6	Verify that the following ports are open to allow for automatic spam, virus and license key updates and Web component access: • Port 80 for HTTP • Port 443 for HTTPS • Ports 31804, 31805 and 31806 (for the Web components)

License key

Verify that you have your license key. If you do not yet have one, please contact your Vircom Sales Representative at sales@vircom.com.

Installing modusGate

Overview

The installer includes the following three components:

1. The server application, including the email gateway services and the Administration Console.

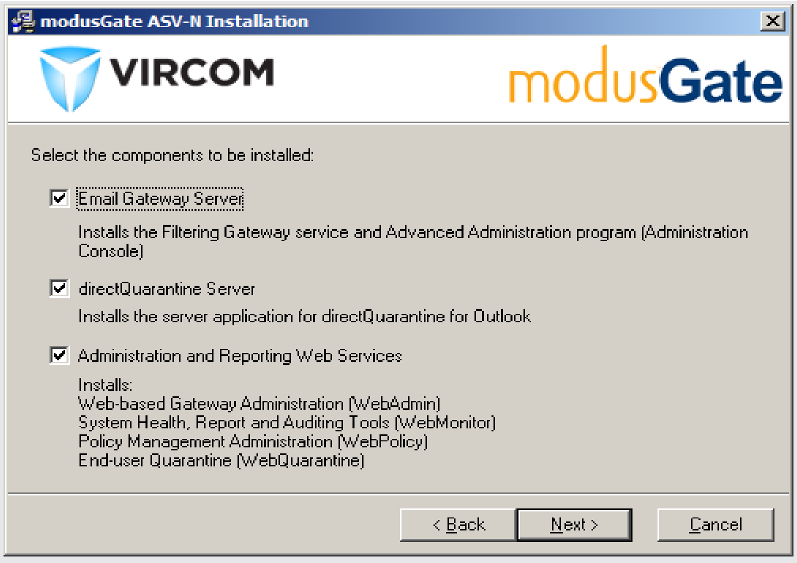
2. The directQuarantine server application, which enables users to access and control their quarantined messages from within Outlook. This is an add-on program that is licensed separately; but is available for trial purposes and fully licensed users.

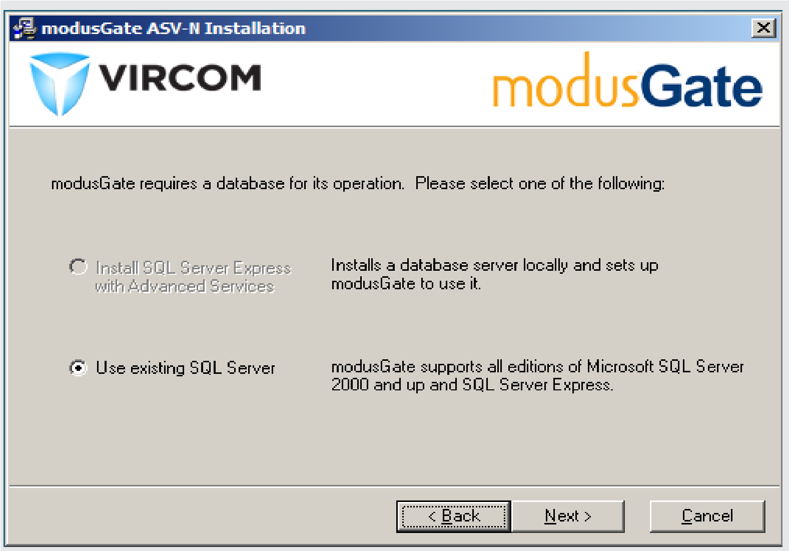
3. The web components, including WebQuarantine, WebMonitor, WebAdmin and WebPolicy (if applicable to your license). These can optionally be installed on a separate web server.

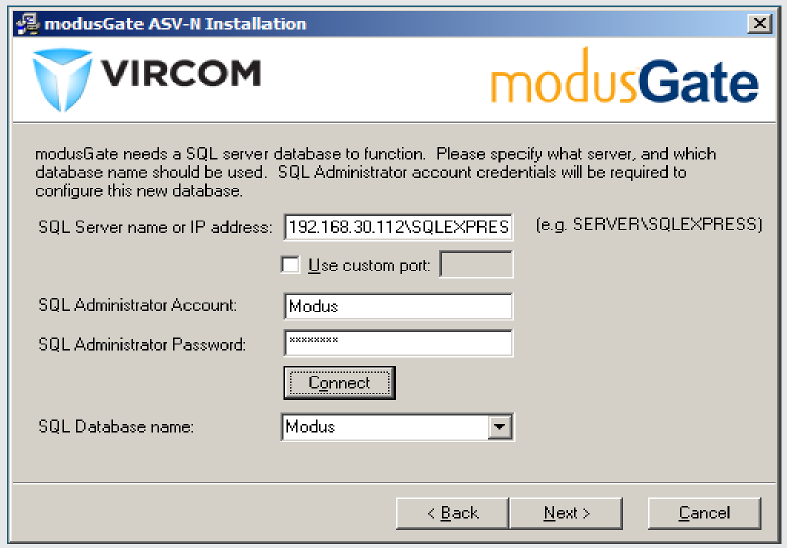
Install modusGate server

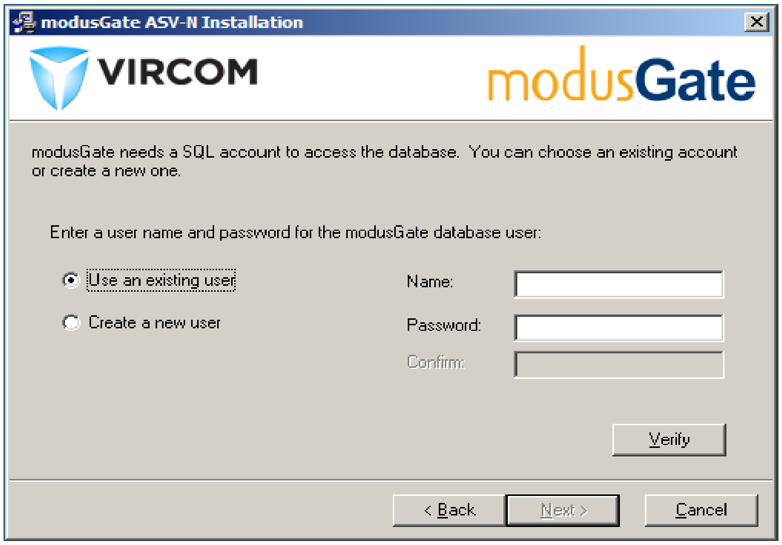
Follow the procedure below to install the modusGate Server application:

Step	Action
1	Log into the server using an Administrator account.
2	Click the .exe file to launch the installation.
3	Accept the licence agreement and click Next to enter your license key. Click Validate > Next.
4	Choose a Standard or Custom install: Select Standard to install all components on the local server, including the server application, directQuarantine and the web components. See the Custom options in Step 5, otherwise continue at Step 6.

Step	Action
5	Custom allows you to select which components to install or disable, and provides advanced settings for database configuration. If the web components are to be installed on a separate web server, select Custom and uncheck Administration and Reporting Services. See “*Installing the web components separately” on page 24* for installation and configuration details. If you plan to use directQuarantine, take note that it must be installed on the same server as modusGate.  modusGate ASV-N Installation Select the components to be installed: ☑ Email Gateway Server Installs the Filtering Gateway service and Advanced Administration program (Administration Console) ☑ directQuarantine Server Installs the server application for directQuarantine for Outlook ☑ Administration and Reporting Web Services Installs: Web-based Gateway Administration (WebAdmin) System Health, Report and Auditing Tools (WebMonitor) Policy Management Administration (WebPolicy) End-user Quarantine (WebQuarantine)
6	Click Next to verify the installation paths. Make any changes necessary and click Next to continue.

Step	Action
7	If you have a SQL Server on the local machine or network, select Use existing SQL Server.This option is automatically selected if a connection can be detected. If you do not have a SQL Server, select Install SQL Server Express with Advanced Services. Clicking Next will direct you to the Microsoft download site to launch the SQL installer. NOTE You must manually restart the modusGate installer after the SQL setup completes and continue with Step 8.  modusGate ASV-N Installation modusGate requires a database for its operation. Please select one of the following: ○ Install SQL Server Express with Advanced Services — Installs a database server locally and sets up modusGate to use it. ● Use existing SQL Server — modusGate supports all editions of Microsoft SQL Server 2000 and up and SQL Server Express.

Step	Action
8	Click Next to enter the SQL Server connection details: • SQL Server name or IP: if using SQL Express, include \sqlexpress after the IP or name. Do not enter spaces either before or after the backslash (\). • SQL Administrator Account: enter the SA account name (or one with equivalent rights) and the Password. • Click Connect to both test the database connection and get the list of existing database names. • Database name: select where to install the modusGate databases. Either choose an existing name from the dropdown menu or enter a new name and click Next.  modusGate needs a SQL server database to function. Please specify what server, and which database name should be used. SQL Administrator account credentials will be required to configure this new database. SQL Server name or IP address: 192.168.30.112\SQLEXPRES (e.g. SERVER\SQLEXPRESS) □ Use custom port: SQL Administrator Account: Modus SQL Administrator Password: ******** SQL Database name: Modus

Step	Action
9	This screen only appears during a Custom install:  modusGate ASV-N Installation VIRCOM modusGate Verify < Back Next > Cancel modusGate needs a SQL account to access the database. You can choose an existing account or create a new one. Enter a user name and password for the modusGate database user: ● Use an existing user ○ Create a new user Name: Password: Confirm: - Select Use an existing user and enter the credentials. - Or, select Create a new user and enter a new name and password: this will be used as the administrator account for modusGate's databases. This option is recommended for security purposes, and modusGate will automatically configure the required permissions in SQL. Click Verify to create and/or validate the user credentials.
10	Click Next to launch the modusGate installation and to create the database tables. This process will take a few minutes.
11	Click OK to start the modusGate and IIS services. NOTE At this point you might be prompted to enter a DNS Suffix: enter your domain name. If this step is necessary, Windows Server will require a reboot to register this change.
12	Delivery failure notices: if the DNS Suffix prompt does not appear, you will instead be asked to provide an email address for delivery failures. This must be a valid address the primary mail server: it is recommended to use your postmaster address.
13	Clicking Next will launch both the Route Wizard and the **What's Next** HTML page containing configuration guidelines.

Configuring routes

Using the route wizard

After modusGate is installed, the **Route Wizard** launches automatically to quickly and easily guide you through setting up the connection (or route) to your mail server.

If you have multiple domains and/or mail servers, or if your mail server type is not specified in the dropdown list, it is recommended to configure the settings manually: click the Switch to Manual button to close the Route Wizard, and follow the directions in the next section, “*Using the console: Connections” on page 19*.

Step	Action
1	Enter your Domain name.
2	Select the appropriate Mail server type from the dropdown list. If your server type is not listed, select SMTP, SMTP_VRFY, or click the Switch to Manual button and use the Console Connections screens to configure your settings. Please note the following important issues: • The SMTP option cannot validate mail recipients, therefore invalid addresses will be created in the user list and count against your user license. In addition, if alias email addresses are used, they will be added to the user list and total user count. • SMTP_VRFY is supported by most mail servers, but must only be used if the mail server is protected by a firewall with no direct public access. Without a firewall, the list of valid user accounts can be easily obtained over the Internet. Alias email addresses are supported by SMTP_VRFY; they will not be counted against the user license.
3	Enter the Mail server name or IP.
4	The SMTP Port number automatically displays 25; change this only if you use a different number. If your mail server type is either SMTP or SMTP_VRFY, click Next and go to Step 9 for the remaining instructions. If you had selected Exchange as the mail server type, click Next and enter your Active Directory/LDAP server information.
5	Enter the Server name or IP address for your Active Directory or LDAP server.

Step	Action
6	Verify the Port number: • If using Exchange 2000-2010, port 3268 is automatically configured for the Global Catalog: this provides access to the entire list of users' mailboxes. Selecting Use SSL/TLS will auto-reset the port to 3269. • If using Exchange 5.5, LDAP port 389 is set. • You may optionally enter a custom port.
7	The Base DN is auto-filled according to the domain name entered in the previous screen. It uses a format supported by both Active Directory and LDAP. EXAMPLE If the domain name is xyz.com, the Base DN format is: DC=xyz,DC=com.
8	User DN and Password: enter the email address and password of the Administrator or mgate user (as instructed in *"Exchange / Active Directory configuration" on page 10*). This format is supported by both Active Directory and LDAP. Please note the following: • It is recommended to use the mgate account: its access to user information is restricted and therefore more secure. • If the mgate user has not been created yet, enter the Administrator's information temporarily. Keep in mind that the user credentials should be updated manually after the account is created.
9	Click Next to view the summary table and verify the information. Click Add to enter other domains or mail servers, if necessary. To edit or change any information, use the Console's Connection settings. Click Finish to close the wizard.

Using the console: Connections

Use the modusGate Administration Console settings:

Step	Action
1	Click on the modusGate icon on your desktop to launch the **Administration Console**.
2	Click Connections, go to Routes > Add Domain.

Step	Action
3	Enter your domain name in Domain mask and click OK • Keep the Route for incoming mail setting: this is required when configuring modusGate with a local (internal) mail server. • Route for outgoing mail is only used if connecting to a mail server that is external to your network.
4	Click Add Route: enter the IP or machine name of your mail server. Do not change the port number unless your mail server uses a different SMTP port. Click OK to display the Properties screen: the server's IP/name and port number are displayed in the Route mail to host or IP address and Port boxes.
5	Automatically populate user list: this is an authentication method that checks if the recipient address exists on the mail server or not, and dynamically populates the Users list as mail flows through modusGate. All methods offer this security except SMTP. Choose one of the following: • SMTP: use this only if none of the other options apply. This is the least secure method as no authentication can be performed, thus invalid addresses will be created in the user list and count against your user license. Alias addresses are also unsupported and will be created as additional users. – When selected, the adjoining boxes to the right should contain the same IP/hostname and port as those entered in Step 4. • SMTP_VRFY is supported by most mail servers, but must only be used if the mail server is protected by a firewall with no direct public access. Without a firewall, the list of valid user accounts can be easily obtained over the Internet. – SMTP_VRFY is safe to use if only modusGate can connect to the mail server. Alias addresses are supported. – When selected, the adjoining boxes to the right should contain the same IP/hostname and port as those entered in Step 4. • Exchange 2000-2010: address validation does occur and aliases are supported. Take note that distribution lists do count as mailboxes. – In the right-hand boxes, enter the IP of the Active Directory (AD) Server if different from the Exchange server. Use port 3268 for access to the Global Catalog (the entire user list), or enter a custom port. You may optionally check Use SSL/TLS.

Step	Action
5 cont'd	• Lotus Domino: supports SMTP_VRFY so consider this option before trying to implement an LDAP-based solution. – Aliases may not be detected when using LDAP and may count as mailboxes. • OpenLDAP: is a generic LDAP auth mechanism that works with many mail servers. – Aliases may count as mailboxes. – In the right-hand boxes, enter the IP of the LDAP Server, if different from the mail server. Use port 389 or enter a custom port. You may optionally check Use SSL/TLS. • Disabled is an advanced option, used to lock the user list and prevent invalid addresses from being dynamically created. This is typically used if Active Directory/LDAP cannot be used for mailbox validation. – The user list must be populated in advance, either manually or by using SMTP until the list is complete. • Exchange 5.5: Using this option requires configuring custom attributes to be used with LDAP and is therefore not recommended. It is preferable to use SMTP_VRFY instead, which must be configured on the Exchange server: – Open the Registry Editor on the Exchange 5.5 Server – Go to HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ MSExchange \ Parameters – Right-click and select New > DWORD value – Enter EnableVRFY – Double-click EnableVRFY > Value data and enter 0x1
6	Authentication Requests: this is required to validate the login credentials to access the WebQuarantine and WebMonitor programs. This setting must be consistent with what was selected for Automatically populate user list. The servername/IP and port fields must also match the settings above: • Use SMTP Auth if either SMTP or SMTP_VRFY was selected above • Use Exchange 2000-2010 if selected above. • If OpenLDAP was selected above, you may choose either OpenLDAP or SMTP Auth. • POP3 is used only in rare circumstances if SMTP Auth is not supported by your mail server. If selected, you must also enable Strip domain name from Authentication requests.

Step	Action
7	If you had selected **Exchange** or **OpenLDAP** in Step 5, complete the LDAP Identification section: • Base DN enter your domain name using this format: DC=*domain*,DC=*com.* EXAMPLE The domain is xyz.com, enter DC=xyz,DC=com • User DN and Password: enter the email address and password of the Administrator or mgate user (as instructed in the Getting Started > Exchange Server xx on page xx). This format is supported by both AD and LDAP. – It is recommended to use the mgate account because its access to user information is restricted and therefore more secure. – If the mgate user has not been created yet, enter the Administrator's information temporarily, and then change it in the console's Connection screen afterward.
8	Repeat the above steps, if required, for each additional domain or mail server.

Test the connections

After configuring a domain and route, perform a telnet test to confirm that the connection works. Use the following instructions:

Step	Action
1	On the modusGate server, go to a Command Prompt (Start > Run, type cmd <enter>)
2	At the command prompt, type telnet xxx.xxx.xxx.x 25 <enter>, where xxx = the modusGate IP address
3	Type helo x <enter>
4	Type mail from: xxx@xxx.com <enter>, where xxx = a legitimate sender's email address
5	Type rcpt to: yyy@yourdomain.com <enter>, where yyy = an email address on your domain
6	Type data <enter>
7	Type subject: this is a test <enter>
8	Type from: xxx@@xxx.com <enter>, where xxx = the same email address previously entered
9	Type to: yyy@yourdomain.com <enter>, where yyy = the same email address previously entered
10	Type testing 1 2 3 <enter>
11	Type . <enter> [Enter a single dot (.) and click <enter>]

Step	Action
12	Type quit <enter>
13	Verify that the recipient address received the message.

Change the MX record

Once your connection(s) are tested and working, the next step is to change your DNS records.

- On the DNS Server, modify the **MX** (Mail Exchange) record so that your mail domain points to the modusGate server instead of the Exchange.
- Create an **A** or Host record that maps the new modusGate MX to the Gate server's IP address
- Since new MX records can take anywhere from 12 to 48 hours to propagate, only remove the mail server's MX after modusGate's MX has been propagated. Do this to hide your mail server from public view: when spammers see multiple MX's for the same domain, they often bypass the primary (modusGate's) and target the secondary (the mail server).

Installing the web components separately

Install the web components

The following instructions apply only if you plan to install the web components on a separate server from modusGate. You will need a copy of your modusGate installation file and the modusGate license key.

Step	Action
1	Log into the server using an Administrator account.
2	Copy the modusGate .exe file to this server and click to launch the installation.
3	Enter the same license key you used on the modusGate server and click Validate > Next. NOTE The license key must match that of the modusGate server or the web components will not work.
4	Select Custom and ensure that only Administration and Reporting Services are selected.
5	Verify the installation path and click Next. Note that all web files will be installed together. Click Next to complete the installation.
6	Follow the instructions below to ensure that each of the web components communicates properly with modusGate.

Modify the web configuration files

WebQuarantine

Step	Action
1	Open Windows Explorer to the **...Vircom\Web\Quarantine** directory.
2	Locate the **WebMailSvr.ini** file and open it with Notepad.
3	Locate the host=xxx.xxx.xxx.xxx and verify that it shows the IP address of the local (Web) server.
4	Locate the SmtpServer=xxx.xxx.xxx.xxx address and change this to the IP of the modusGate server The POP3 and IMAP address default to the localhost; leave these as is (they are not used)
5	Locate DomainName=machine_name.mydomain.com: change this to match the primary domain as it appears on the modusGate Console
6	Save the changes.

WebMonitor

Step	Action
1	In Windows Explorer, go to the **...Vircom\Web\WebMonitor** directory.
2	Locate the **custom.config** file and open it with Notepad.
3	Locate <add key="Servers" value="localhost"></add>: replace localhost with the IP address of the modusGate server.
4	Save the changes.

WebAdmin

Step	Action
1	In Windows Explorer, go to the **...Vircom\Web\WebAdmin\Root** directory.
2	Locate the **web.config** file and open it with Notepad.
3	Locate <add key="Site" value="" /> and enter modusGate's IP address between the empty quotes.
4	Open **Administrative Tools > Services** and restart the WEBMAILSVR service.
5	Restart the IIS service to register the collective changes for all the web components.

Configure the ODBC connection

Step	Action
1	On the server that now houses the web components, go to Start > Administrative Tools > Data Sources (ODBC).
2	Click System DSN > Add.
3	Select the driver that matches your database type and click Finish. - For SQL Server 2005 Express: select SQL Native Client - For all other SQL versions, select SQL Server.
4	Enter a name for the connection and the SQL Server address (can be the IP address or hostname). For SQL Express, enter *servername\sqlexpress*. Click Next.
5	Select SQL Server authentication and enter your login credentials, e.g. the *SA* account and password. Click Next.
6	Select the modus database and click Next.
7	Click Finish and Test Data Source to confirm a successful connection.

SECTION 4

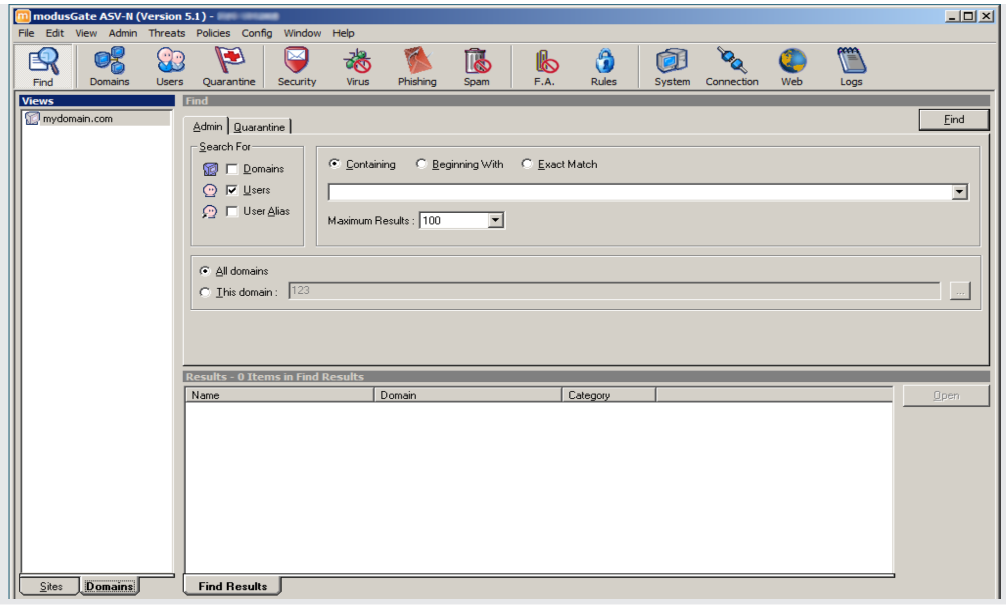
modusGate Administration

The administration console

The Administration Console is designed to provide a high level of flexibility and control over the modusGate server configuration. It gives you the option to set system-level parameters that can be applied to all users, or to customize particular settings for select domains and/or users who require special mail handling rules.

Navigating the console

To navigate through modusGate, click on the Toolbar buttons at the top of the console. You will then find a series of tabs or panels within each screen.



modusGate ASV-N (Version 5.1) - [redacted]

Views: mydomain.com

Find — Admin | Quarantine

Search For:
- □ Domains
- ☑ Users
- □ User Alias

● Containing ○ Beginning With ○ Exact Match

Maximum Results : 100

● All domains
○ This domain : 123

Results - 0 Items in Find Results

Name	Domain	Category

Views

The Sites View displays the machine name where modusGate is installed.

The Domains View lists the domains for which modusGate is filtering and/or relaying mail.

- The list of domains (if multiple) is created dynamically once the Connections or routes have been configured and mail begins to flow through modusGate.

- Double-clicking a domain name in the Domain view will display the properties panels for that domain. (Note that clicking the Domains button in the toolbar will produce the same behavior.)

Users

- The list of users is also created dynamically once mail begins to flow through modusGate.

- Click the Users button in the toolbar: the results window will display all usernames in a given domain. If there are multiple domains, click the domain name to see the list of users for that domain.

- Double-clicking a username in the results window will display the properties panels for that user.

NOTE Please note the following exceptions regarding the Users list:

- The Users list and property panels are not accessible when using modusGate with an unlimited user license.

- The Users list will not populate dynamically if, in the Connections screen, you set Automatically populate user list to Disabled.
  - This is an advanced option used for special configuration requirements, and/or to prevent automatic cleanup of unused mailboxes during the regular synchronization process.

Override functionality

To support customization, override settings are available in the domain and user properties for the following features: alias addresses, footers (or disclaimers), audit logging, and filter controls (where applicable), including language preferences for the Quarantine Report and the WebQuarantine interface.

NOTE Overrides do not apply to an **unlimited user license.** Because Domain and User level properties are not stored on the local server in this format, overrides are unavaillble in the Administration Console.

Server Level

- Configuration changes made at the server level are propagated to all domains and users.

- Users and domains are able to override settings unless Forced options are enabled (i.e. for scan functions).

Domain Level

- Configuration changes made at the domain level affect all users within that domain.

- Domain-level settings will override the server settings **if** permission to override was granted.

User Level

- Configuration changes affect only the individual user.

- User-level changes override the server and domain settings **if** permission to override was granted.

In general, modusGate checks for and applies settings in this order: 1) User, 2) Domain, and 3) Server.

Exceptions to this rule do exist and will be highlighted where applicable.

System

This following sections in this document describe the configuration options and recommended settings for each of the Toolbar panels, beginning with the core System settings.

NOTE Any references to scanning, filtering and quarantine operations in the following sections do not apply to the modusGate L version. The availability of spam and virus operations depend on your license.

Services

From this panel, you can start, stop and configure the modusGate services:

- Click on a service to select it
- Click on Start, Stop or Settings
- If Settings is not available, the configuration cannot be modified for this service

These services can also be started and stopped in the Administrative Tools > Services panel, and are set to start automatically.

SMTPRS

The SMTP Receiver Service is responsible for performing the following actions:

- Receiving all incoming email from the Internet.
- Applying all security settings on incoming messages and either accepts or blocks them according to your rules.
- Performing mailbox validation to ensure that the message recipient has a valid account on your system. When the address is invalid, the message is rejected, thus reducing the load on the mail server.

Click Settings to configure the Transmission and Submission ports:

Transmission: the standard port is 25. This is the port used by external mail servers to communicate with your server. Do not change this port unless you do port mapping via a proxy server or firewall.

Submission: this port is used when local users are configured to send outbound mail through modusGate to the Internet. The standard port used for this purpose is 587.

- You can configure your mail server to use port 587 to route outbound mail to modusGate for scanning prior to delivery to the destination addresses, or configure the users' mail client settings to use port 587 as the SMTP server port.

SMTPDS

The SMTP Delivery Service is responsible for the following actions:

- Relaying mail to your mail server for local delivery to the mailboxes.
- Handling mail for delivery to external (non-local) email addresses.
- Processing only the messages that have passed security and content checking.

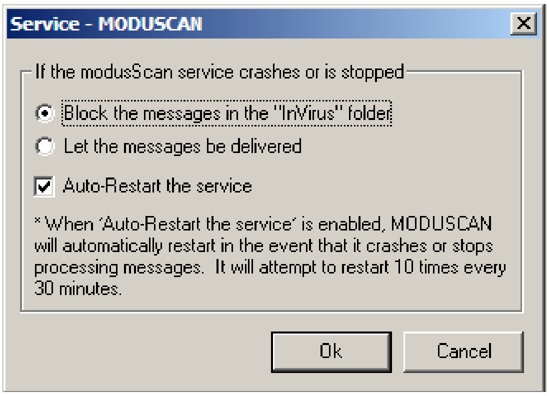
Click Settings to configure an IP address for outbound messages, if necessary. This is only used if you use separate IPs for incoming and outgoing mail traffic.

MODUSCAN

The modusGate Scanning Service does the following:

- Handles messages after they have been verified and accepted by the SMTPRS/security checks.
- Runs attachment, spam scanning and/or virus scanning, where applicable.
- When spam and/or dangerous content is found, it handles messages according to your preferences, e.g. quarantine, delete or ‘tag and pass.’
- If messages are considered legitimate, they are passed to SMTPDS for delivery.

Click Settings to configure the auto-restart options. If MODUSCAN should stop for any reason, these settings determine what happens to new, incoming messages:



Service - MODUSCAN

If the modusScan service crashes or is stopped

● Block the messages in the "InVirus" folder

○ Let the messages be delivered

☑ Auto-Restart the service

* When 'Auto-Restart the service' is enabled, MODUSCAN will automatically restart in the event that it crashes or stops processing messages. It will attempt to restart 10 times every 30 minutes.

Block the messages in the ‘InVirus’ folder will store new, unscanned messages in the message queue until the service restarts.

When this option is enabled, Auto-Restart the service must also be enabled. This ensures that potentially dangerous messages do not bypass the scanner.

Let the messages be delivered will ensure that mail continues to flow whether MODUSCAN is running or not, however it will also potentially allow dangerous content to get through.

MODUSADM

This is the server administration service, responsible for automatic updates of the spam and/or virus engines, filter definitions and the quarantine database. It is also responsible for a number of internal functions.

MODUSMON

This service is used by the WebMonitor application to provide updated server statistics and maintain the monitoring database.

MODUSCFG

This service is used by the Policy Management (WebPolicy) application, if applicable. It is required to provide access to WebPolicy and to communicate with Active Directory.

MODUSDQ

This is the directQuarantine server service, which provides end users with a live view of their quararantined messages in Outlook and the content controls.

WEBMAILSVR

This service controls the WebQuarantine server service, if installed on the modusGate server. When the web components are installed on a separate machine, the service appears stopped (this is normal behavior).

Summary: message processing sequence

This is a very brief overview of how modusGate processes messages:

1. A sending mail server opens a connection to modusGate.

2. The SMTPRS service responds, requesting the sending server's identification and the message header details.

3. SMTPRS then applies all configured security checks to validate the supplied information. If the message fails any security criteria, or if the recipient address does not exist on the local system, the connection is rejected and closed.

4. Message transmission begins after passing all security criteria.

5. The MODUSCAN service then begins scanning the message (according to applicable options).

6. If the message fails the scan, it is treated according to the handling rules.

7. If the message is clean, it is then passed to the SMTPDS service for delivery/relay to the mail server.

Scanning order

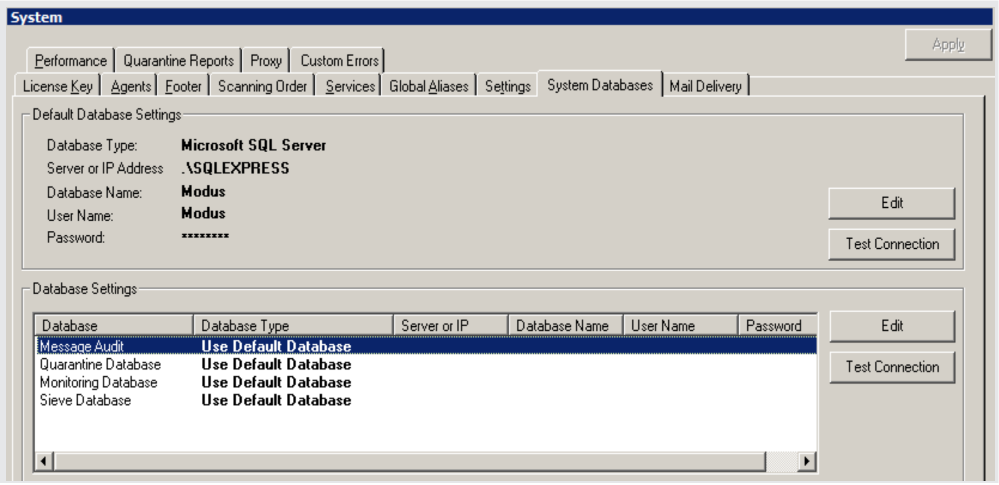
modusGate is configured to scan messages for Forbidden Attachments prior to scanning the content for Viruses. This order is designed to reduce processing load on the server and increase the speed of message handling.

You may optionally reverse this order, but you must stop and restart the MODUSCAN service to register this change.

System databases

Multiple databases are configured automatically during the modusGate installation. These include the Message Audit, Quarantine, Monitoring and Sieve (containing Vircom's spam definitions and any custom filters you might create). All are stored in the "Default" location, however settings can be modified for individual databases.

EXAMPLE If you have a large number of mailboxes on your system (e.g., 500 or more), you should create a separate Quarantine database to ensure better peformance.



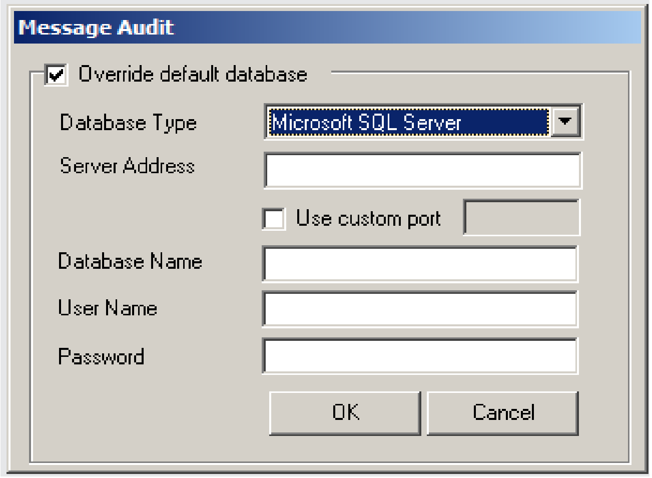
Default Database Settings

Database Type: Microsoft SQL Server
Server or IP Address .\SQLEXPRESS
Database Name: Modus
User Name: Modus
Password: ********

Database Settings

Database	Database Type	Server or IP	Database Name	User Name	Password
Message Audit	Use Default Database				
Quarantine Database	Use Default Database				
Monitoring Database	Use Default Database				
Sieve Database	Use Default Database				

If you wish to modify a particular database, follow the steps below:

Step	Action
1	Select the database name and click Edit.
2	Enable Override default database, if applicable. (Note that the Default database can also be modified and has its own Edit controls.)  Message Audit ☑ Override default database Database Type: Microsoft SQL Server Server Address: ☐ Use custom port Database Name: User Name: Password: OK Cancel
3	Use the dropdown menu to select the Database Type. The menu will display different options depending on the database format supported. NOTE Access and Postgres (PostgreSQL) are considered legacy platforms and are no longer recommended. In addtion, if you plan to use the Greylisting feature in the Security settings, the Default database must be SQL: neither Access nor Postgres is supported.
4	Enter the Server Address: use either the IP or server hostname.
5	Enable Use custom port if necessary. modusGate dynamically determins the port for SQL Server, but change it manually if it is incorrect.
6	Enter the new Database Name.
7	Complete the User Name and Password fields. If this account does not yet exist on the database server, the necessary access rights will be configured automatically.
8	Click OK to create the new database structure. NOTE If you wish to move or copy data stored on the 'old' database, this must be done manually using the SQL Server import/export controls.
9	**Optional:** click Test Connection. This option can be used at any time to verify that modusGate is able to communicate with the database server

Extended Database

If you use a Blockade configuration of two or more modusGate servers, Vircom provides the Extended Database structure to store Users' properties.

The database script can be found in the modusGate program files: ...\Vircom\modusGate\DBStructures\SQL Server\ExtendedDB.

For up-to-date information about the database schema and the various properties, see the Knowledge Base:

http://kbase.vircom.com/kbase/default.asp?id=1710&SID=&Lang=1

Quarantine Reports

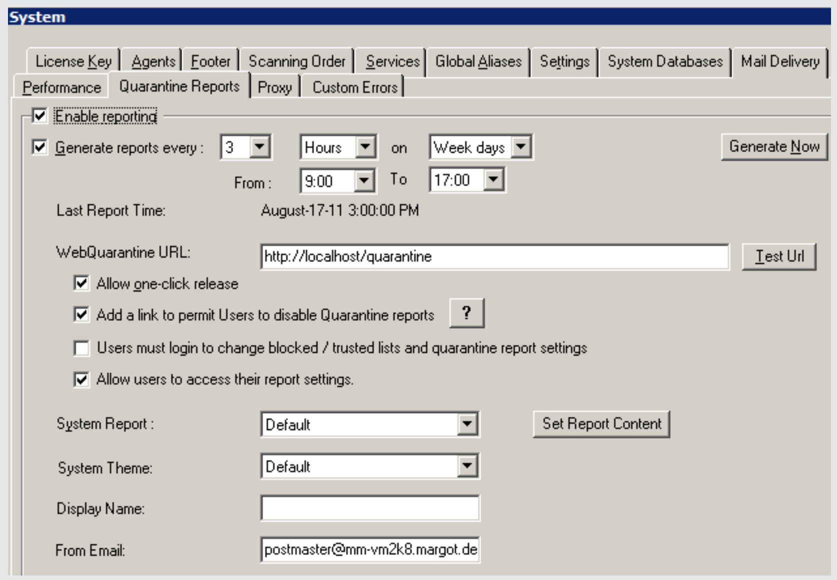
modusGate provides the option to send quarantine reports to your users. The report is a summary digest that is emailed on a scheduled basis.

Links within the report allow users to release or delete spam, add sender addresses to their trusted or blocked lists, and in some cases release forbidden attachments (with special permission).

If a user releases a message containing a forbidden attachment, it is scanned for viruses (where applicable). Consequently, the message could be quarantined again, in which case it cannot be released through the report.

NOTE Reports will not be generated in the following cases: a) for people who have disabled reporting, either at the domain or user levels and b) when no new spam, viruses or attachments have been caught since the previous report was generated.

To configure quarantine reports for the entire system:

Step	Action
1	Select Enable reporting.  System License Key Agents Footer Scanning Order Services Global Aliases Settings System Databases Mail Delivery Performance Quarantine Reports Proxy Custom Errors Generate Now Test Url ? Set Report Content ☑ Enable reporting ☑ Generate reports every : 3 Hours on Week days From : 9:00 To 17:00 Last Report Time: August-17-11 3:00:00 PM WebQuarantine URL: http://localhost/quarantine ☑ Allow one-click release ☑ Add a link to permit Users to disable Quarantine reports ☐ Users must login to change blocked / trusted lists and quarantine report settings ☑ Allow users to access their report settings. System Report : Default System Theme: Default Display Name: From Email: postmaster@mm-vm2k8.margot.de
2	Enable Generate reports every and set the desired frequency. Note that the minimum hourly schedule is 3 hours: this limit reduces the potential performance impact on the server.
3	If WebQuarantine is installed on the modusGate server, the WebQuarantine URL should display http:/localhost/quarantine. If WebQuarantine is installed in a separate server, enter the URL as above, but replace 'localhost' with the web server's IP. Or, if you prefer, enter the web address according to your configuration in IIS, e.g., http://www.mycompany.com/quarantine.
4	Click Test to ensure that a "*URL test successful*" message appears in a web browser on the modusGate server. The test must succeed for the quarantine reports to function properly.

Step	Action
5	Select from the following access control functions: Allow one-click release: allows users to release their quarantined mail using the links within the Quarantine Report. Add a link to permit Users to disable Quarantine Reports: allows users to opt out of receiving the Quarantine Report. • To enable this function, you must first go to the Web section of the console > Allowed User Properties> Edit, enable Reporting Frequency and click Apply. Users must login to change blocked/trusted lists and quarantine report settings: this forces users to authenticate before making any changes to these settings Allow users to access their report settings: provides a link in the Quarantine Report that provides users with direct access to their settings in WebQuarantine.

Step	Action
6	You may change the following report format settings, if desired: System Report: is the master layout for the Quarantine Report. You may optionally create a custom report, which can then be selected from the dropdown menu. System Theme: you may optionally customize the colors, fonts, logos, etc., used in the Quarantine Report. Use this setting to select a custom theme. NOTE For information about creating custom reports, see the Knowledge Base article: http://kbase.vircom.com/kbase/default.asp?id=1720&SID=&Lang=1 Display Name: enter the email address to be displayed in the From: field in Quarantine Report messages. From Email: enter the email address to be used when sending the reports. By default, the postmaster address is used.
7	Set Report Content: these settings determine what message details are included in each user's Quarantine Reports. The default settings provide the maximum amount of information. A note about the spam probability levels: this feature can be used as a filter to display only the messages that may have been quarantined in error (i.e., False Positives). It is recommended to select the Medium and Low probabilities for this purpose. • Messages labelled High probability can safely be disabled for most people. **Optional:** You can allow users to set their own report content preferences by enabling permission: • In the Console, go to Web > Privileges > Allowed User Properties > Edit, enable Reporting Content and click Apply. • Users will then have access to these settings by logging into WebQuarantine, and can make any desired adjustments.

Domain controls: Quarantine Report

Override settings for the Quarantine Report language and content controls are also available in the Domain properties in the Console:

- In the toolbar, click Domains > select the domain name > Reporting. Enable Override server default settings, and make any necessary adjustments.
- In the Domain tab, enable Override to select a language for the Quarantine Report. The default is English.

User controls: Quarantine Report

Override settings for the Quarantine Report language and content controls are also available in the User properties in the Console:

- In the toolbar, click Users > select the user name > Reporting. Enable Override domain default settings, and make any necessary adjustments.
- In the General tab, enable Override to select a language for the Quarantine Report. The default is English.

License Key

This panel provides important information about your license key, including the expiry date, your current build and patch versions, and the number of licensed users.

Validate: any license changes authorized by Vircom, such as product renewal, increasing users, purchasing add-on programs, etc., are updated via your license key and validated automatically by system. Validate can be used to manually update changes, but it is not necessary to do so.

Browse: use this function to locate and select your license key text file if doing a manual validation.

The Users section displays the current number of licensed users and how many seats remain available. An automatic process runs daily to synchronize the user names between modusGate and your authentication server (such as Active Diretory/LDAP), and to remove any invalid addresses or those that are no longer active on the authenication server.

NOTE In some cases, administrators flag certain mailboxes as inactive on the authentication server but must continue to keep and/or receive mail for them. These addresses may be automatically removed by modusGate's synchronization process. To prevent their removal from modusGate, do the following:

- In the Console, go to Users > select the username that must be kept
- In the General properties tab, enable Keep this user permanently > Apply.
- You may optionally use Disable Account to stop message filtering but keep the account in place.

Synchronize Now: can be used to manually synchronize the user names.

Threshold Warning: modusGate issues a warning notice when the number of users approaches 95% of the limit allowed by your license. You may adjust this threshold to receive these warnings earlier (using a lower percentage, e.g., 80%) or later (using a higher percentage, e.g., 98%).

EXAMPLE if the maximum number of mailboxes is 500 and the threshold is set to 95%, a warning message appears when there are 475 users on your system.

Footer

From this panel, you can enter footer or disclaimer text to be inserted at the end of every outbound message sent from the mail server.

To use this feature, you must configure your mail server to route outbound messages (i.e., to non-local email addresses) through modusGate.

Domain controls: Footer

Footer settings can be customized per domain:

- Go to Domains > domain name > Footer. Enable Override default message settings and Append this message to the end of each outgoing message.
- Enter your text, select Format and click Apply.

User controls: Footer

Footer settings can also be customized per user:

- Go to Users > user name > Footer. Enable Override Domain Default Settings and Append this message to the end of each outgoing message.
- Enter your text, select Format and click Apply.

Settings

This panel contains general server settings, such as the directories for the mail spool and system logs.

Mail Spool Directory: this is the location of the message spool or queue.

The spool can optionally be moved to another drive on the modusGate server, but placing it on a network shared drive is not recommended. If you move the spool, you must enter the new directory here, and stop/restart all modusGate services.

NOTE The spool must not be placed on a separate server from modusGate.

System Log Directory: this is the location of the system logs, such as operational and error logs.

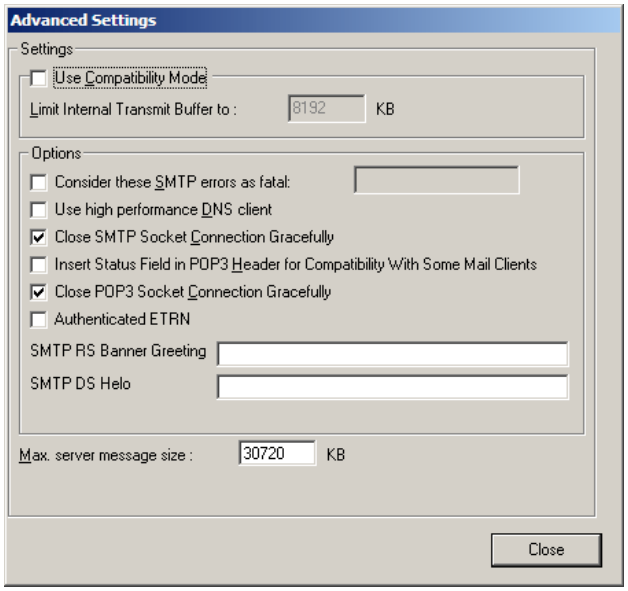
This directory can be moved to another drive, including a network shared drive. If you move the log directory, you must enter the new location here and stop/restart all modusGate services.

Language: used to select the language for the Quarantine Reports. The default is English.

The language can be customized per domain (see **Domain controls: Quarantine Report**) or per user (see **User controls: Quarantine Report**).

Send delivery failure notices to this email address: displays the email address entered during installation, if enabled. You may change this address at any time.

Advanced options:



☐ Use Compatibility Mode

Limit Internal Transmit Buffer to : 8192 KB

☐ Consider these SMTP errors as fatal:

☐ Use high performance DNS client

☑ Close SMTP Socket Connection Gracefully

☐ Insert Status Field in POP3 Header for Compatibility With Some Mail Clients

☑ Close POP3 Socket Connection Gracefully

☐ Authenticated ETRN

SMTP RS Banner Greeting

SMTP DS Helo

Max. server message size : 30720 KB

Use Compatibility Mode: Do not enable - this setting does not apply to modusGate.

Consider these SMTP errors as fatal: when enabled, you can specify a list of numerical error codes, separated by a comma (,). When modusGate encounters one of these errors from a another server, it will bounce the message immediately without attempting to resend it.

Use high performance DNS client: if the default DNS client is too slow when performing reverse DNS lookups, an alternate (high performance) DNS client can be used instead.

Close SMTP Socket Connection Gracefully: use this option if modusGate experiences problems with SMTP sockets that remain in an indefinite WAIT state. This setting will enable modusGate to close the sockets.

Authenticated ETRN: when enabled, an SMTP client must first be authenticated through the AUTH command with a valid mailbox name and password before using the ETRN command.

Reject messages with empty bodies: certain types of spam messages are sent with empty bodies and are therefore missing the final single dot that signals the end of transmission. Using this setting blocks such messages and prevents processing issues on modusGate.

SMTPRS Banner Greeting: use this option to create a custom banner greeting, if desired. This greeting is seen by external mail servers when they initiate a connection to modusGate.

SMTPDS HELO: this setting enables you to modify how your domain name appears in the HELO line when sending messages to another server.

Max server message size: this value sets the maximum message size (in KB) that the server will accept. A value of ‘0’ denotes no message size limit.

Mail Delivery

This is the message delivery schedule: a list of time intervals when modusGate attempts to resend mail that could not be delivered successfully. Time is measured from the moment message delivery fails to when the next attempt is made.

Messages are kept in the modusGate spool or queue while delivery is retried at each interval listed. If the final time is reached, the message is deemed undeliverable and returned to the sender. Times marked with an envelope icon indicate when a notification is generated, informing the sender that the message has not yet reached its destination.

The retry frequency can be modified by adding or removing intervals. This is especially useful if/when your mail server goes offline for any reason. The final time can be increased (e.g., from 2 days to 4 or more) to ensure that messages to your users remain stored on modusGate until the mail server is back online.

Click Add to enter a new time interval to the list.

Select an interval and click Remove to delete it from the list.

Use Send Warning/No Warning to enable/disable sender notifications at a specific time.

If an unusually large number of messages begin queuing for a particular domain, you can attempt to force delivery using one of two methods:

Force automatic retry for these domains: Click Domain List, enter the domain name(s) and set a Retry count: this will be the total number of retry attempts.

Enter the domain names for immediately delivery: enter the domain name(s) or a wildcard in the text box and click Deliver Now.

NOTE Neither of these methods guarantee delivery. Serious connection issues can occur on the recieving end that prevent successful delivery.

Global Aliases

This feature allows you to create global aliases for your system, such that mail sent to one address can be redirected another. For example, you want mail addressed to domainA.com to be redirected to domainB.com.

When not to use Global Aliases

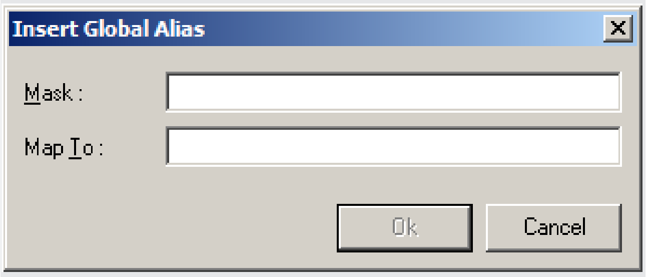
You should note that this is a legacy feature that has been kept to support certain older systems that require it. Alias settings exist in both the Domain and User properties, which are recommended for use instead. See **Domain controls: Aliases** and **User controls: Aliases**.

Do not use this feature if any of the following situations apply to you:

- You plan to enable Quarantine Reports for your users.
- You have aliases already configured on your mail server, and your routes are configured to use either SMTP_VRFY or Exchange/Active Directory. These aliases are usually detected and added to the users' properties automatically.

Configuring Global Aliases

Should you need to use this feature, follow the directions below:

Step	Action
1	Click Insert to add an alias.  EXAMPLE You want mail addressed to domainA.com to be redirected to domainB.com.
2	Enter the alias address in Mask, i.e., domainA.com from the example above. Wildcards are accepted, e.g.,*@domainA.com.
3	Enter the destination address in Map To, i.e., domainB.com from the example above and click OK. This must be an actual address on the system: it cannot be an alias. Wildcards are accepted, e.g., *@domainB.com.
4	Use the Up and Down buttons to set the priority. Aliases are processed in the order listed. Wildcards must be placed at the end of the list.

Step	Action
5	**Optional:** use Import to populate the list using a text file. You must enter a single alias/destination pair per line using the format, **mask address : map to address.** Enter a space before and after the colon (:). EXAMPLE domainA.com : domainB.com
6	Use the Find button to search the list. Wildcards are supported.

Domain controls: Aliases

Domain alias names can be configured in the console:

- In the toolbar, click Domains > select domain name > Aliases.
- Click Add, and enter the alias name.
- Aliases are used when you want mail addressed to domainA.com to be redirected to domainB.com. These addresses must exist on your system.

User controls: Aliases

User alias names can be configured in the console:

- In the toolbar, click Users > select user name > Aliases.
- Click Add, and enter the alias name.
- Aliases are used when you want mail addressed to userA@domain.com to be redirected to userB@domain.com. These addresses must exist on your system.
- Depending on your alias configuration in Exchange/Active Directory, user aliases are usually detected automatically and dynamically created in the Console.

Agents

An Agent calls an external program, such as a script or batch file, that runs every time the server receives a message. It can be used to redirect, copy (archive) or to delete messages.

NOTE If your modusGate version supports the use of sieve scripts, it is recommended that they be used instead of agents, especially when archiving messages. Agents process messages before content filters are applied, thus messages containing malware will also be archived.

Please see the following Knowledge Base articles for more details:

1. When to use sieve scripts vs. agents:

http://kbase.vircom.com/kbase/default.asp?id=1561&SID=&Lang=1

2. How to write a mail agent:

http://kbase.vircom.com/kbase/default.asp?SID=&Lang=1&id=1316

To create an agent, follow the directions below. The example given will archive all inbound and outbound messages that pass through modusGate:

Step	Action
1	In the Agent text box, type the name of the batch file or program to be run, followed by %m %r • The %m directive copies the message file • The %r directive copies the header envelope • Be sure to enter the full path to the file name with quote marks (“”) EXAMPLE "C:\Progra~1\Vircom\modusGate\ARCHIVEMAIL.BAT" %m %r Click Apply.
2	Open Notepad to create your batch file. Click Save As and enter the filename from Step 1 (e.g., archivemail.bat). Save the file to a folder in the system path, e.g., "C:\Progra~1\Vircom\modusGate\...”
3	Enter the following text: @ECHO OFF FIND /I "@domain.com" %2 > nul IF %errorlevel% == 0 COPY %1 C:\AnyDestinationFolder\ NOTE modusGate only supports the ability to direct messages to a specified folder, not a mailbox

Proxy

If modusGate is installed on a network that is configured to access the Internet through a proxy server, you must enter the proxy server information in this panel. This is required to access the spam engine and anti-virus updates.

Click Use a proxy server and enter the host or IP address and the port of the proxy server.

Custom Errors

From this panel, you can create custom error messages for each of the Error types listed in the dropdown menu. If nothing is entered in these fields, the default error messages are used.

Custom error messages will only appear in your own error logs. External servers receive only default errors.

Preferences

These settings enable you to configure how long to cache SMTP authentication information for modusGate. This allows validated senders to maintain open connections to the server for the time you set before having to re-authenticate.

Cache Size: specify the number of entries to keep in cache.

Cache Entry lifetime: specify the number of seconds to keep the cache entry.

Keep SMTP Connection Alive For: specify the number of seconds to keep the connection open.

Security

Security overview

modusGate's security tools provide full flexibility to prevent spam attacks and security breaches on your mail system. Every security feature was designed to help businesses maintain system integrity.

All security settings affect the system as a whole: they cannot be modified per domain or per user. Please follow the guidelines and proceed with caution when modifying the settings. If you have any questions or need further details, please do not hesitate to contact our Support Team at support@vircom.com.

Using address lists (mask lists)

In most of the following features where address lists are created, you can use wildcards and other formatting to accelerate the process of entering IP addresses, host names and email addresses. Supported formats include:

Mark	Means
*	The wildcard (*) denotes inclusion, i.e. use all variations of the entry. EXAMPLE To block all yahoo.com addresses, enter *@yahoo.com. This format is accepted in all lists, except where specified.
!	The exclamation mark (!) denotes an exclusion, i.e. use all entries except this one. This format is accepted in most lists, except where specified.
/xx	CIDR (slash) notation or netmask. This format is supported by all features where IP addresses are entered, to denote and include subnet masks. EXAMPLE 192.168.42.23/24

The order of entries in the lists is important, as modusGate applies rules from the top of the list downwards. To set the priority of a specific entry, use the Up or Down buttons.

Most features allow you to create and store text-based lists elsewhere on the server and to specify the file location in the feature settings, without having to manually recreate the list in the console. However, doing so may cause performance issues, particularly if lists are quite long. It is therefore recommended to import list contents into the console to speed up response times. Lists may be updated and reimported at any time, overwriting the previous lists with the updated entries.

Protocol Filter

The protocol filter allows you to block email messages based on header content. This filter comes enabled and pre-populated with several known header formats that have been used in past attempts to bypass various security measures.

While this feature is most useful for modusGate L and AV versions where sieve scripts are unavailable, it is recommended to leave the filter operational and intact for all modusGate versions.

How the filter works

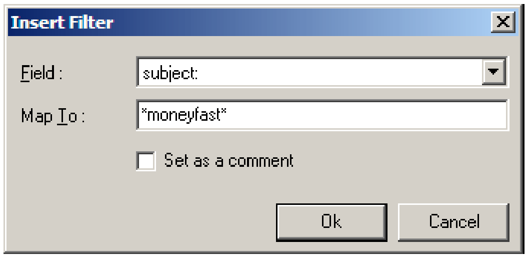
There are two parts of an email - the envelope and the header - that contain the sender, recipient and other address information. The envelope is deleted when the message is delivered successfully. The header is part of the message (it can be viewed in the mail client). In the envelope, the sender field is mailfrom and the recipient is rcptto. The equivalent fields in the header are from and to, respectively.

The protocol filter is used by specifying a list of text strings that correspond to the envelope/header content to be rejected. All incoming messages are checked against the filter list, and a message gets rejected when a matching entry is found.

Because the envelope and header addresses can differ, it is good practice to a) use wildcards, and b) create duplicate strings for the mailfrom/from and rcptto/to pairs.

NOTE The filter file name must be SPAMFLT0.TXT and must be located in your modusGate™ directory.

To add a new filter string:

Step	Action
1	Click Insert to add a new string  Insert Filter Field : subject: Map To : *moneyfast* □ Set as a comment
2	In the Field box, select the element to be filtered.
3	In the Map To box, enter the string you want to block. Use wildcards (*) to block variants of the string. EXAMPLE You want to block subjects like “Make money fast” Enter *money fast* This will capture messages containing random characters before and after the subject (a trick to evade filters).

Step	Action
4	Click OK to save the entry and repeat the process to create as many entries as necessary.
5	Optional: Set as a comment inserts a pound sign (#) to tell the filter to ignore that particular string.
6	Use Edit to change an existing filter.
7	Use the Up and Down buttons to change the priority: filters are applied in order from top to bottom.
8	Stop and restart the SMTPRS service to register any changes.

SMTP Security

This panel provides several SMTP authentication mechanisms.

Force authentication for these IP addresses:

- Used to specify a list of IP addresses required to use SMTP authentication when relaying email.
- It forces users to authenticate prior to sending mail through modusGate. Users must have SMTP Auth enabled on their mail clients. Without authentication, message transmission will be blocked.

Do not advertise SMTP Auth (for these IPs):

- SMTP Auth is normally ‘advertised’ or displayed as an available authentication method when the EHLO command is issued in the message header. Spammers can potentially hack users' accounts by collecting passwords that are transmitted to the server in clear text via PLAIN or AUTH LOGIN mechanisms. It is recommended to use this feature and to enter ***.*.*.***
- Used to support email clients who force the use of SMTP Auth when they see SMTP Auth as advertised.

NOTE When authenticating via SMTP AUTH, the authentication is only valid for the current SMTP session. Once the session is closed, for subsequent attempts, the same user will not be authenticated by default. This eliminates the possibility of spoofing.

Force usage of fully qualified addresses in SMTP commands

- The system will reject messages that do not use a proper email address format (e.g. user@domain.com) in either the mail from: or rcpt to: fields
- This feature helps to block mass-mailed messages sent to unspecified addresses or <Undisclosed Recipient>.

Reject malformed addresses

- Used to reject messages where addresses are not contained within angled brackets (<>) in either the mail from: or rcpt to: fields, e.g., <user@domain.com>.

- Standardized email clients such as Outlook, Outlook Express and Netscape support this format.

Validate Sender Addresses

- Performs a reverse DNS check on the sender’s address.

- Recommendation: set Cache Size to 9000, and Keep in Cache to 240

Enable Bounce Address Tag Validation (BATV)

BATV checks for backscatter spam (or misdirected bounces). Backscatter occurs when a mail server receives spam and legitimate email, and sends bounced messages to the recipient. However, with spam, the original MAIL FROM field usually contains a legitimate (but forged) email address. During a spam wave, a mail server may generate bounces to the forged MAIL FROM addresses, thus redirecting the mail to the legitimate email address who is the real target of the spammer. This could result in the server's IP address being placed on DNS blacklists.

When BATV is enabled, SMTPDS adds an encrypted tag to the MAIL FROM field of all outgoing messages. If a bounce returns without a tag, then we know it did not originate from modusGate. The message is either rejected or quarantined (depending on your settings).

Additionally:

- Validation is performed after the RCPT TO command so that messages are blocked before their content is transferred

- If an address is invalid, modusGate processes it as a permanent failure by returning a 550 response to the SMTP command containing the address.

- If a message is identified as a bounce and not BATV validated, SMTPRS will return a 550.5.7.5 error code:

  BATV uses the following format: Tag Type = Tag Value = Loc-core
  E.g.: prvs=13266C8ED1=John@domain.com

  The Tag Type is "prvs" (private simple signature)
  The Tag Value is in the format KDDDSSSSSS

  BATV uses the following format: Tag Type = Tag Value = Loc-core
  E.g.: prvs=13266C8ED1=John@domain.com

  The Tag Type is "prvs" (private simple signature)
  The Tag Value is 13266C8ED and is unique for every message sent
  The Loc-core is the mailfrom address John@domain.com
  The Loc-core is the mailfrom address John@domain.com

Apply BATV checking when the message contains matching subect tags from this list

- Click Subject Tags to enter a list of commonly used subject tags (e.g., out of office) to reduce the likelihood of false-positives.

- Use only one entry per line.

- Do not use commas (,) to separate entries as they are forbidden characters.

Disable BATV for these IP addresses

Click IP Addresses to enter IP addresses or IP classes for which BATV will not be used.

NOTE When enabled, modusGate sets a default grace period of 7 days. During this time, no messages are filtered using BATV to prevent improper handling of older messages. BATV filtering begins when the grace period ends.

For more information about BATV, see:

http://tools.ietf.org/html/draft-levine-smtp-batv-01

Mail Relay

This feature allows you to specify which IP addresses or domains are allowed to relay mail through your server, preventing your server from being used as an open relay.

Mail Server Cloaking

- This hides the mail server from public view when relaying mail for a defined route.

- modusGate becomes the public-view server.

Accept mail for relay...from these hosts

- Enter the IP addresses and domain names that are allowed to send mail through the server (i.e. to external addresses).
- The localhost address (127.0.0.1) and the IPs corresponding your configured routes are automatically added to this list.
- When adding addresses, accepted formats are: 10.10.10.10, 10.10.10.*, 10.10.10.0/16, and *domain.com*.

Block Scan Attack

This feature allows you to limit the number of recipients per incoming message. This effectively prevents spammers from sending messages with an unusually high number of recipients. You can also prevent dictionary spam attacks by slowing them down or blocking them.

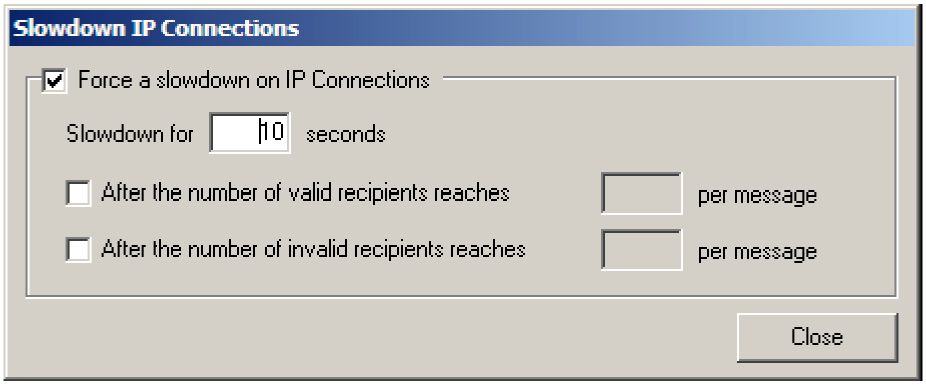
- To exclude specific IP addresses from this limit, go to Security > Trusted Address List > SMTP Security Trusted Address > Trusted Address, and enter the IP addresses.

Limit the Maximum Number of Valid Recipients

- Allows you to limit the number of recipients per message accepted by SMTP.
- The message will be rejected if the number of recipients exceeds this limit.

Slowdown the IP Connections

- When the set message threshold is reached, a slowdown is enforced between each subsequent message from the sending IP.
- Enter the number of seconds for which the connection will be slowed.
- Enter the number of valid and invalid recipients per message, after which the connection will be slowed.



Slowdown IP Connections

☑ Force a slowdown on IP Connections

Slowdown for 10 seconds

□ After the number of valid recipients reaches per message

□ After the number of invalid recipients reaches per message

Block IP Addresses

- Used to block IP connections that violate the threshold.
- Enter the number of minutes for which the connection will be blocked.
- Enter the number of valid and invalid recipients per message, after which the connection will be blocked.
- To prevent a dictionary spam attack, use the Block IP option and enter a low number (3-5) for **invalid recipients**.

NOTE The Slowdown the IP Connections and Block IP Addresses settings should not be used at the same time. The ‘Slowdown’ settings will override and disable the ‘Block’ settings.

Caching

- Set the maximum cache size.
- Enter the maximum number of IP addresses that will be kept by the system. When the maximum is reached, the oldest IP entry in the cache will be removed.

Maximum Entry Life Time

- Enter the lifetime of an entry in the cache.
- When the maximum is reached, the oldest IP entry in the cache will be removed.

Sender Reputation

Sender Reputation System (SRS)

This is Vircom's own RBL service (reputation.vircom.com).

SRS classifies email based upon who is sending the message rather than its contents. Upon establishing a connection to the SMTP receiver service, a DNS query is made to Vircom's RBL with the IP address of the computer connecting to the service. If the IP address is found in the RBL, that computer is considered to be a spammer. The connection can either be dropped immediately or the message from that sender can be quarantined.

Vircom's RBL differs from other RBLs in that it is highly dynamic. It is updated every few minutes, based on who is sending the most spam to our honeypots. Similarly, if someone spams our honeypots accidentally, they will automatically be removed from the list a few hours after they stop spamming.

Sender Validation: Greylisting

Basic Mode (default): modusGate sends a temporary error to the sender after the DATA command in the SMTP protocol exchange.

- Upon receipt of a temporary error, a valid SMTP-compliant mail server will resend mail. By contrast, spam-sending zombies are unlikely to resend mail.
- Basic Mode provides a strong defense against text and image spam. In fact, because the temporary error is sent before the body of the message is received, this mode does not discriminate if the message contains text or image spam.

Vircom Extended Mode (recommended): modusGate sends a temporary error to the sender after the END of DATA command CRLF.CRLF.

Extended Mode is designed to protect against spam and is intended to work in conjunction with Vircom's SCA™ engine. While the SCA engine is very effective at blocking image spam, the speed with which spammers create variants of their images has required us to increase our spam blocking efforts.

How it works

A spam tactic is to send 1000's of copies of a single image spam, containing randomly modified versions of the image, during a short period of time. Spammers do this by taking advantage of a delay between the time the new image spam variant is detected and the time it takes Vircom to create a new signature for the image. In as little as a few seconds, before new signatures can be created, the spammer can count on at least a small percentage of the variant image spam making their way to the users' inboxes.

The extended mode adds protection by reducing the window of opportunity that the spammer uses to send variants of image spam:

- When the first image spam is received, a signature is created for the message and cached.
- The message is not accepted. Instead, a temporary error is returned to the sender. This blocks a significant number of image spam because few spammers will resend.
- If the message is re-sent, a signature is created for this message.
- The signatures of the first and second messages are compared. Valid senders always resend the same message; therefore the signatures will be identical and the message will be delivered. By contrast, a spammer is unlikely to resend the exact same message. In the event that a spammer sends a second message (albeit a different one), modusGate will respond to it in the same manner as it did for the first and the message will be cached. Assuming an identical message is never resent within the cache time frame (i.e. 4 hours by default), the sender's IP address will be added to the blocked senders list.

Extended Mode is designed to protect against spam and is intended to work in conjunction with Vircom's SCA™ engine. While the SCA engine is very effective at blocking image spam, the speed with which spammers create variants of their images has required us to increase our spam blocking efforts.

Differences between Basic and Extended Modes

Basic Mode (how greylisting is normally implemented) cannot block messages where the spammer resends it using the same Mail From: and RCPT TO: pair.

Extended Mode will block messages if there is any modification to the content. It will not be activated if the spammer resends the exact same message.

Because Extended Mode is only activated when the message body contains an image, this causes fewer delivery problems for local users.

Regardless of the mode used, the following are not subject to greylisting:

- Trusted IP Addresses (Trusted Address List, Authenticated via POP/IMAP Auth Senders or SMTP_AUTH.)
- Senders whose domain has a SPF record but only if SPF Support is enabled (see SPF Support below.)
- Sender's IP address if found during a whitelist lookup but only if the feature is enabled (see Perform a lookup for SMTP host in the Real-Time Whitelist servers.)

Greylisting database information

- To support greylisting, the default database (see System > System Databases) must be configured to use SQL Server. No other database formats can be used.

- Greylisting database records are automatically expired after 8 hours.

Log Entries

Greylisting will generate two types of log entries in the **OPR** (Operations) log:

1. "Message from <Sender's IP> was temporarily rejected because of greylisting policies."

- This is the most common log entry, indicating that the sender was given a temporary error.

2. "Message from <Sender's IP> was rejected because of greylisting policies."

- This log entry only occurs when message is not re-sent within the default 4-hour time-frame. Failure to re-send within a 4-hour limit results in blacklisting the IP address for a 4-hour period.

Sender Validation: SPF support

Sender Policy Framework helps detect email sent with faked or forged sender addresses. SPF support only works for those domains that put SPF definitions in their DNS.

For more information about SPF, see http://www.openspf.org/.

Perform a look up for the SMTP host in the DNS

- Enables Reverse DNS lookup: this allows you to check if the IP of the sender's server resolves to the given domain name.

- This option is processor-intensive: you should monitor system performance when using it.

Reject Connection Immediately On Lookup Failure: when enabled, messages are rejected when the reverse lookup fails. This setting works together with the Lookup Timeout: the connection can also be rejected when the DNS lookup reaches the specified timeout limit.

Postpone the rejection until authentication: modusGate looks for an SMTP AUTH connection before performing the reverse lookup

Do not reject connection (Accept all hosts): the results of the DNS lookup are logged, but the message is processed whether the lookup fails or not.

To exclude IP addresses from Reverse DNS, add them to the Security > Trusted Address List > SMTP Security Trusted Address settings.

Perform a lookup for SMTP host in the Real-time Whitelist Servers

- Enable any of the specified Real-time Whitelist servers available for use with modusGate.
- If the sender's server information is approved by the Whitelist servers, it bypasses the modusGate connection settings. However, the content is still subject to spam and virus scanning (if applicable).

Real-Time Blacklist

This feature allows you to connect to a Real-Time Blacklist (RBL) to verify if mail senders are blacklisted. RBLs are 3rd party databases that contain lists of IP addresses belonging to known spam sources. modusGate checks incoming mail against these RBLs, and if a sending server's address is found on any of the lists, its mail will be blocked.

Select the RBL servers where the look up will be made

- Click on RBL Servers to enter the IP address or DNS server name for the RBL(s).
- RBLs can be aggressive and may cause legitimate mail to be blocked from entering your mail system. For a list of recommended RBLs and their aggression levels, see:

http://kbase.vircom.com/kbase/default.asp?id=1553&SID=&Lang=1

Select the host IP's that will be excluded from the look up

- IP Exclusion: enter the IP addresses that will bypass the RBL lookup.
- If you must allow email from an RBL-listed server, add its IP to the exclusion list to ensure mail delivery.
  - Alternately, add the IP address to Security > Trusted Address List > SMTP Security Trusted Address.

Reject connection immediately if the host is blacklisted: RBL runs at the beginning of the connection and blocks any server found on the list(s). This option is recommended to optimize speed.

- If disabled, the connection will only be severed after the RCPT TO command.

Perform RBL check after mailbox authentication: modusGate waits until the sender's email address can be validated through SMTP Auth before determining whether to block the server or not.

- This benefits users who may have legitimate accounts in modusGate but whose sending IP addresses are listed on an RBL. With this setting, modusGate first verifies the address and accepts and processes mail only if it is legitimate; otherwise, the connection will be closed.

Caching: Allows you to specify how many RLB lookups will be kept in cache and for how long.

Possible RBL connection issues

Using RBLs may affect system performance, therefore you should monitor the server when using this feature.

Vircom has no affiliation with any RBL nor does it have control over their content and availability. If an RBL goes down or is no longer in service, mail flow will slow down or may be halted entirely (as no DNS resolution can occur). Vircom is never warned of issues with RBLs and, as such, cannot notify its clients.

To troubleshoot a possible RBL problem:

Step	Action
1	Open the RBL Server list, click Export, and copy and save your list to a text file.
2	Click Remove to delete all addresses from the list. Click Close and Apply.
3	Go to System > Services. Stop and restart the SMTPRS service.
4	From a command prompt, telnet to port 25 to check the banner response (it should be immediate).
5	Using your saved RBL text file, re-enter each address, one at a time, into to the modusGate list. Click Apply, and perform the telnet test after each entry.
6	When the problem RBL has been identified (i.e. banner response is not immediate), remove that entry and stop/start SMTPRS.

Connection Limits

This feature allows you to limit the number of simultaneous SMTP connections allowed from a single IP. This also controls performance as it limits the number of users that can use your system at a given time.

Total number of connections allowed for this server

- Used to specify the total number of simultaneous SMTP connections allowed on your server at one time.
- The default is set to 500.

Total number of simultaneous connections allowed from the same IP

- Used to specify the number of simultaneous connections allowed from one IP address.
- The default is set to 10.

Maximum connection rate allowed for this server

- Used to limit the total number of connections allowed per second.
- The default is set to 50.

Maximum simultaneous connection rate allowed from same IP

- Used to limit the number of new connections allowed per second, per IP.
- The default is set to 10.

Connections

These settings allow you to block connections from specific IP addresses. If a user has been identified for abusive email practices, he/she can be prohibited from using the mail system.

Reject all incoming mail from these hosts

- Enter the addresses to be prohibited from sending mail to your server. Both IP addresses and domain names can be entered here.

Reject all incoming mail from these addresses

- You can use this list to enter specific email addresses to be blocked from sending mail to your server.

Trusted Address List

These settings allow you to enter the IP addresses that are considered “trusted” or allowed by your mail server.

SMTP Security Trusted Address:

Mail sent from the IP addresses entered here bypass the following list of security checks. This affects both inbound and outbound messages, therefore you should limit the list to internal and well-known sources only.

- Block Scan Attack
- Reverse DNS
- Real-Time Blacklist
- Banned IP Addresses
- Connection Limits
- SPF
- Greylisting
- Protocol Filter

NOTE IP addresses entered here must also exist in the Mail Relay > Accept mail for relay from these hosts field.

Scanning Trusted Address:

This setting is available only to the modusGate versions that provide spam scanning. It is used to allow mail from local IPs to bypass all spam scanning (including custom rules) on **outgoing** mail bound for the Internet. Virus and attachment scanning, if available, will not be bypassed.

Incoming Internet mail will continue to be scanned according to your configuration.

NOTE IP addresses entered here must also exist in the Mail Relay > Accept mail for relay from these hosts field.

Encryption & Certificates

Use this panel to configure encryption and certificate settings to add an extra level of protection to your mail system.

Encrypt Message Transmission

Using certificates will ensure that your mail transmission connections are protected against unauthorized access. Different certificates can be used per domain or IP to ensure unique encryption signatures and improve security. Note that this method protects the communication channel between servers, but not the message content.

To use this feature, you must first purchase server certificates. For more information, visit company websites such as www.thawte.com, www.verisign.com or www.entrust.com.

Use the following directions to configure modusGate to use certificates:

Step	Action
1	Purchase and install the server certificate(s) according to the issuer's instructions. NOTE Certificates MUST be installed in the default local computer account or modusGate cannot use them.
2	In the modusGate console, go to Encrypt Message Transmission > Use certificate. Select the certificate name and click Apply.
3	To assign different certificates to different IPs, click Advanced Certificate Setup > Add. Enter the IP, select the certificate name to be assigned and click OK. Repeat this process for each IP/certificate assignment required.
4	Select Enable SMTP Encryption and click Apply.
5	Stop and restart both the SMTPDS and SMTPRS services.
6	**Optional:** select Force incoming and outgoing encryption for these: IP Addresses to force specific encryption certificates to be used for certain IP addresses. • If you force encryption for SMTP, there may be interoperability problems if the outside server does not use the same type of encryption protocols. • You MUST NOT force encryption on the IP address between the modusGate server and your Web server UNLESS you configure the Web server as a secure site. To do so, continue with the following steps.
7	Install the Web server certificate(s) in the directory of the default local computer account.
8	In Internet Information Services (IIS) Manager, select the default website (or select the specific website for which you want to configure encryption). Right-click and select Properties.
9	Go to Directory Security > Edit.
10	Select the appropriate encryption strength: • Require Secure Channel (SSL): forces users to use a secure connection (HTTPS) when connecting to the modusGate Web application. • Require 128-bit encryption: forces users to use a stronger encryption method.
11	In Client Certificates, ensure Ignore client certificates is selected.

Encrypt Message Content

The Console settings are used ONLY if you have the PGP® Email Gateway server. For configuration details, see the Knowledge Base article:

http://kbase.vircom.com/kbase/default.asp?id=1691&SID=&Lang=1

Sieve script method for other encryption servers

If you use a non-PGP server to encrypt message content and wish to use modusGate to filter outbound messages, contact Vircom's Support team at support@vircom.com. They will help you create a custom sieve script for this purpose.

Domain Keys

From this panel, you can configure DKIM (Domain Key Identified Mail) for modusGate.

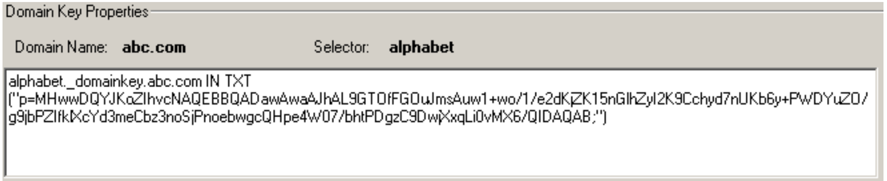
Domain Keys is a method of authentication that uses public keys and the DNS to establish the origin and contents of an email message. It allows for near end-to-end integrity from a signing to a verifying Mail Transfer Agent (MTA) and is independent of SMTP routing.

modusGate can be set to check only inbound messages for a DKIM signature, or optionally to add a signature to outgoing messages.

Enable DKIM for inbound messages: set this option to verify that incoming messages have a valid DKIM signature.

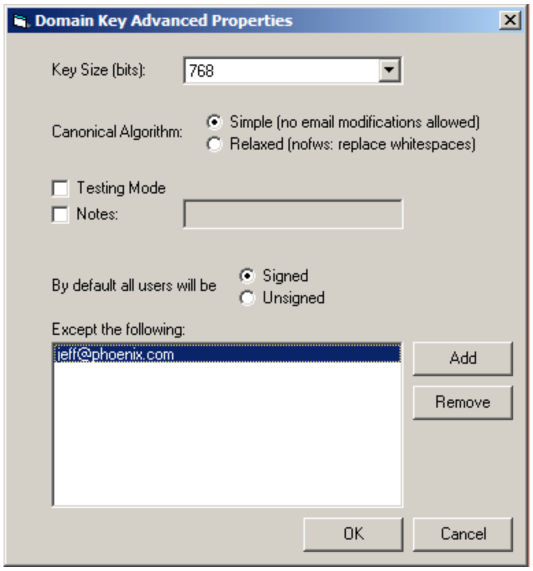
- Unsigned messages will not be blocked: the verification results will be added to the header under Domain Keys.
- Signed incoming messages are identified by one of three domain key statuses:
  - Good: the domain signature was properly verified
  - Bad: the domain signature verification failed
  - Unknown: verification did not occur (e.g. DNS lookup failed, bad signature syntax, etc.)
- No status is given to incoming messages that do not have a signature.

Use the following instructions to configure DKIM signatures on outbound messages:

Step	Action
1	Click Enable DKIM signing for outbound messages
2	**In** Domain Key Configuration**, click** Add.
3	Enter your Domain Name (e.g.domain.com) where indicated.
4	In the Selector box, enter a word of your choice. This will be used as a secondary identifier for the domain. For security reasons, do not use the same word for more than one domain. The Edit button can be used to change the selector, but you MUST also replace the DNS string on the DNS server after doing so.
5	When you click OK, your public key appears in the Domain Key Properties window.  Domain Key Properties Domain Name: **abc.com** Selector: **alphabet** alphabet._domainkey.abc.com IN TXT ("p=MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAL9GTOfFGOuJmsAuw1+wo/1/e2dKjZK15nGlhZyI2K9Cchyd7nUKb6y+PWDYuZO/g9jbPZIfkIXcYd3meCbz3noSjPnoebwgcQHpe4W07/bhtPDgzC9DwjXxqLi0vMX6/QIDAQAB;")
6	The public key string must be copied into your DNS text record. Click Export string to copy the string to a text file. Follow the steps below to configure the DNS record.
7	NOTE These instructions are specific to Microsoft DNS Server, but should be similar for other DNS servers: Open the DNS Server console and expand Forward Lookup Zones**.**
8	Right-click the domain and select New Domain.
9	In New DNS Domain, enter _domainkey and click OK.
10	Right-click _domainkey and select Other New Records.
11	In Resource Record Type, select Text (TXT) > Create Record.
12	In Record Domain, enter a name for the record (e.g. DKIM).
13	In the Text field, paste the public key string copied from the the modusGate Console.

Step	Action
14	If using **Microsoft DNS**: do NOT copy the parentheses or the quotation marks (see example below): p=MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAO0kPmcqXXdTVieTo YfhIA2HdoT/ k4P5aoj0bHnZgNrP24jaOZ1TKYE+QsdSTOJE5blqSNie7alGMC+y/ VrKW907dMCZyY3Rnwa08dStII9VAfr2Of/Z6i8bW/ YAExnvRHQIDAQAB; If using **Bind DNS**, you MUST use the parentheses and quotation marks.
15	Exit the DNS Server console and return to the DKIM panel in modusGate.
16	Click Test DNS String. If you had created strings for multiple domains, select a domain name first in the Domain Key Configuration table before clicking Test DNS String.
17	If the test is successful, click Enable to activate the signature.
18	To delete a signature, select the domain name and click Remove. You must also remove the DNS string from the DNS server.

Advanced settings:



Domain Key Advanced Properties

Key Size (bits): 768

Canonical Algorithm:
● Simple (no email modifications allowed)
○ Relaxed (nofws: replace whitespaces)

□ Testing Mode
□ Notes:

By default all users will be
● Signed
○ Unsigned

Except the following:
jeff@phoenix.com

You can optionally use this panel to modify the key structure:

NOTE Any changes made to the following properties will change the DNS string. Therefore, you must also replace the string text on the DNS server.

Key Size: use this to optimize performance (default is 768 bits).

- Larger numbers will reduce performance but will increase the difficulty of breaking the signature.

Canonical algorithm: used to determine how the header is handled:

- Simple (default): tolerates almost no modification of the email message in transit.
- Relaxed: tolerates common modifications such as whitespace replacement and header field line rewrapping.

Testing Mode: use this feature to signal to the receiving server that you are testing the signature. The receiving server treats unsigned messages with the same importance as signed messages.

- Receiving servers must not treat messages from signers in testing mode differently from unsigned email, even should the signature fail to verify.

Notes: you can add comments to the public key string which will not be interpreted by the receiving server (limit of 265 characters).

- This tag should be used sparingly because the DNS server has space limitations.

Signed/unsigned: you can configure modusGate so that all users are either signed or unsigned.

- You can specify an exception list by clicking Add**.**

How DKIM Works

When a message is sent out through modusGate, DKIM adds a header (DomainKeys-Signature:) that contains a digital signature of the message contents. The receiving SMTP server uses the name of the sending domain, the _domainkey string and a selector from the header to perform a DNS lookup. In turn, the returned data includes the domain's public key. Immediately after the DomainKeys-Signature: header, the receiving mail server decrypts the hash value in the header and recalculates the hash value for the message contents. If the two values are a match, it proves, cryptographically, that the email message originated from the intended domain and that the message was not altered in transit. The way in which forged messages are handled is left to the discretion of the receiving server’s administrator.

While DKIM does not prevent email abuse, it allows abusive domains to be tracked and detected, thus helping to prevent fraud. By identifying the sender's domain, domain-based trusted and blocked senders lists are more effective, as is detecting phishing. The absence of a DKIM signature indicates that email could be forged (i.e. a forged source email address or domain).

Please consult the following RFC for more information:

http://www.rfc-editor.org/rfc/rfc4871.txt.

Content Filters

Overview of content filtering

The following sections describe the content filter controls applicable to modusGate AS, AV and ASV versions.

Each filter type allowed by your license (virus, attachment and/or spam) is enabled system-wide when modusGate is installed, and set to the highest level of security.

Domain and User settings exist for all filter types, except if you have an unlimited license. Scan aggression levels can be configured per domain or per user, providing greater flexibility and user control.

Administrators have ultimate control over all filters, however, through the use of master switches at the system level. These switches allow you to turn filters on or off system-wide, to force certain settings for all users, or to set special permissions for select users.

In general, modusGate checks for and applies the scan controls in this order: 1) User, 2) Domain and 3) Server.

However, custom filters (or sieve scripts) can be configured in the Rules section to run before all scanning, to ensure that user settings do no bypass company policies.

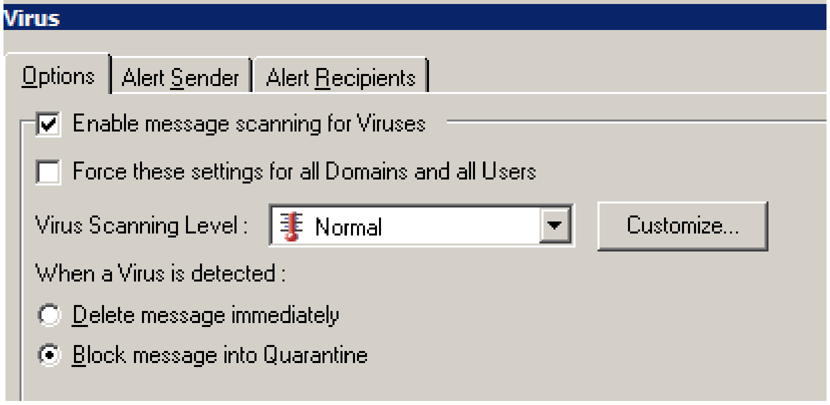
Virus

The Virus controls are separated into 2 layers of tabs: Properties and Preferences (seen at the bottom of the panel). This section begins with the Preference settings, which is where you set the scan levels and message handling rules.

Options

Virus scanning is automatically enabled to scan inbound messages from the Internet. Messages are always scanned for dangerous content prior to spam scanning. For better performance, attachments are filtered first, before viruses, however this order can be changed in the System > Scanning Order settings.

- If you also wish to scan users' outbound email, you must configure your Exchange (or other mail server) to route these message to modusGate prior to sending to the Internet.



☑ Enable message scanning for Viruses

□ Force these settings for all Domains and all Users

Virus Scanning Level : Normal

When a Virus is detected :

○ Delete message immediately

● Block message into Quarantine

Force scanning for all Domains and all Users

- Overrides individual settings for users and domains and forces a virus scan on all messages.
- Do not use this function if you plan to allow domains and users override privileges.

Virus Scanning Level

- Used to select the scanning level: Normal, Customized or Disabled.
- With Customized selected, click on the Customized button to determine the scanning level for viruses and corrupted/unscannable files.

- If Disabled is selected, virus scanning is turned off.

When a virus is detected:

Choose one of the following options when a virus is found:

- Delete message immediately
- Block message into Quarantine

Alert Sender

This feature enables you to specify if and how to notify the sender that the message contained a virus.

CAUTION Due to current behavior of spam and malware that spoof sender addresses, do NOT use this option. If enabled, false notifications are likely to be sent to people who did not actually send the virus.

Alert Recipients

This feature allows you to specify if and how to notify the recipients when a message contains a virus.

NOTE Both directQuarantine and/or Quarantine Reports clearly label the messages that contain viruses, so you may want to use those features instead of the notification process.

Enable Alert Notifications to Recipients

- This must be turned on at the server level to be able to set individual controls at either the domain or user levels.

Recipients receive notification

- This server-level override function allows you to reset individual domains and/or users' settings to force everyone to receive alerts.
- Enter the Name, Address and Subject for the alert messages.

Select the message to be used for the alert:

- Use the default message.
- Use message from file: create a custom TXT or HTML file containing the notification text, and browse to select the file name.
- Use current message (plain text): enter your text in the window below.

Attach cleaned message

- When enabled, a copy of the cleaned message (without the virus) will be sent as an attachment to the notification email.
- If the virus cannot be removed, the message will be quarantined.
- When disabled, the recipient will only receive notification of the email message and the original will be quarantined.

Encoding

- Specify the text format: either Text / plain, or Text / HTML.
- Remember to enter the HTML code in the message body or specify an HTML file if you are pointing to a file.

Alert Substitutions

In the alert notifications, you may use two substitutions that will insert text based on the message being scanned and the results of the scan:

- Insert the sender name of the infected message: enter %1!s!
- Insert the scan report from the anti-virus engine: enter %2!s!

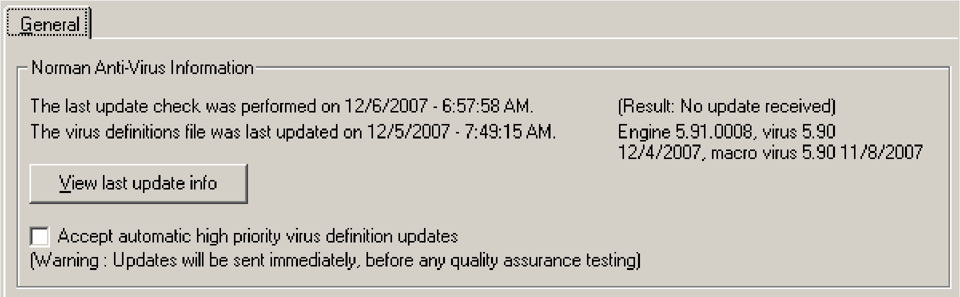
Properties settings

The following sections describe the settings in the Properties tab (bottom of the Virus panel).

Properties provide details about the virus scan engine and the update process.

General

This panel provides general information about the virus scan engine, including the last online, update check and when the last download of the virus definitions occurred.



The last update check was performed on 12/6/2007 - 6:57:58 AM. (Result: No update received)
The virus definitions file was last updated on 12/5/2007 - 7:49:15 AM. Engine 5.91.0008, virus 5.90 12/4/2007, macro virus 5.90 11/8/2007

□ Accept automatic high priority virus definition updates
(Warning : Updates will be sent immediately, before any quality assurance testing)

The information you see in this panel will depend on your licensed version, and may display update details for the Norman® engine, the McAfee® engine, or both.

View last update info

- This opens a text file which provides the URL for new virus signature information on the Norman/McAfee website.

Accept automatic high priority virus definition updates

- Virus definition updates from Vircom are tested for quality. However, there may be emergency situations when the virus definition files are available prior to quality assurance tests.
- If you choose to receive these signature files without waiting for quality assurance testing, check this option and they will be sent to you as soon as they are available.

NOTE It is recommended that you leave this feature disabled unless you require a time-critical update from Vircom. As the files have not passed quality assurance testing, Vircom cannot guarantee that these files will run properly, which may cause system problems.

Auto-Updates

The auto-update feature connects modusGate to a Vircom server to receive updated virus definition files, ensuring that your modusGate server, and your users, are always protected.

Check For Updates Every

- Use the drop-down menu to select when your mail server checks for virus definition files from Vircom.
- The system is automatically configured to check for new definintions every 15 minutes.

Update Now can optionally be used to force an immediate update of the files.

Use a secure HTTPS connection to download the virus definition updates: This feature is not implemented yet.

Auto-Cleanup

These settings allow you to specify when a message is deleted from the virus quarantine.

Messages are removed from both the quarantine folder and the database when the expiry date is reached, or when the maximum total size is reached - whichever comes first.

You may optionally modify these settings:

- Message expires after: enter the number of days.

- Max. Total Size: enter the number of KB.
- Start job at: enter a time using the format hh:mm.

Performance

These settings enable you to set parameters to improve the performance of the anti-virus engine.

Enable Performance Caching

- Performance caching enables modusGate to recognize messages that have previously been scanned for viruses. When a message with the same virus enters the mail system, it is treated like the original.
- Virus scanning does not occur for these messages: they are immediately quarantined or deleted according to your settings.
- This feature is useful when dealing with Internet worms that can send hundreds and thousands of copies to a mail server at one time.
- The infected file is only scanned once but all copies are treated in the same manner as the first one.

Cache Size: Specify the number of entries to be kept in the performance cache.

Keep in Cache for: Specify the lifetime of a cache entry. Once time has expired, the entry will be removed from the cache.

Enable Attachment's size verification

- You can restrict scanning for large attachments (which can potentially slow system performance).
- Enter the maximum file size in KB.

Postmaster

You can optionally specify a Postmaster mailbox to receive notifications when a virus is detected.

- Send Notifications to Postmaster: Enable to enter a postmaster mailbox. This must be a valid address on your mail server.

Domain controls: Virus

Virus settings can be configured at the Domain level in the Console:

Go to Domains > select domain name > Virus

Enable Override server default settings:

- Override cannot be selected if Force scanning for all Domains and all Users is checked in the system settings under Virus > Preferences > Options.
- Configure your preferences for scanning level, message handling and recipient notifications.
- Do NOT enable Senders Receive Notification (see **Alert Sender**).

User controls: Virus

Virus settings can be configured at the User level in the Console:

Go to Users > select domain name > Virus

Enable Override domain default settings:

- Override cannot be selected if Force scanning for all Domains and all Users is checked in the system settings under Virus > Preferences > Options.
- Configure your preferences for scanning level, message handling and recipient notifications.
- Do NOT enable Senders Receive Notification (see **Alert Sender**).

Phishing

Phishing overview

Phishing spam has become more prevalent and, as such, modusGate isolates it as a separate feature. Messages with phishing content are handled like viruses. However, the scan behavior actually mimics that of spam: the definition files are updated by the spam engine and, by default, the update occurs every 15 minutes.

Options

Force scanning for all Domains and All users

- Overrides individual settings for users and domains and forces scanning on all messages.
- Do not use this function if you plan to allow domains and users override privileges.

Scanning Level

- Select the level of aggressiveness for scanning: Disabled, Normal, Strong or Extreme.
- Extreme is set by default, but may produce False Positives. If this occurs, reducing it to Strong should provide a good balance between protection and little-to-no false positives.

When Phishing is detected

Choose one of the following options for message handling:

- Delete message immediately
- Block message into Quarantine

Allow users to release phishing messages

- This enables users to release phishing messages from quarantine in the event of a false positive.
- This feature can be enabled for specific users only, if desired. See the information below.

Domain controls: Phishing

Phishing settings can be configured at the Domain level in the Console.

Go to Domains > select domain name > Phishing

Enable Override server default settings:

- Override cannot be selected if Force scanning for all Domains and all Users is checked in the system settings under Phishing.
- Configure your preferences for scanning level, message handling and whether members of this domain can release phishing messages from Quarantine.

User controls: Phishing

Phishing settings can be configured at the User level in the Console.

Go to Users > select user name > Phishing

Enable Override domain default settings:

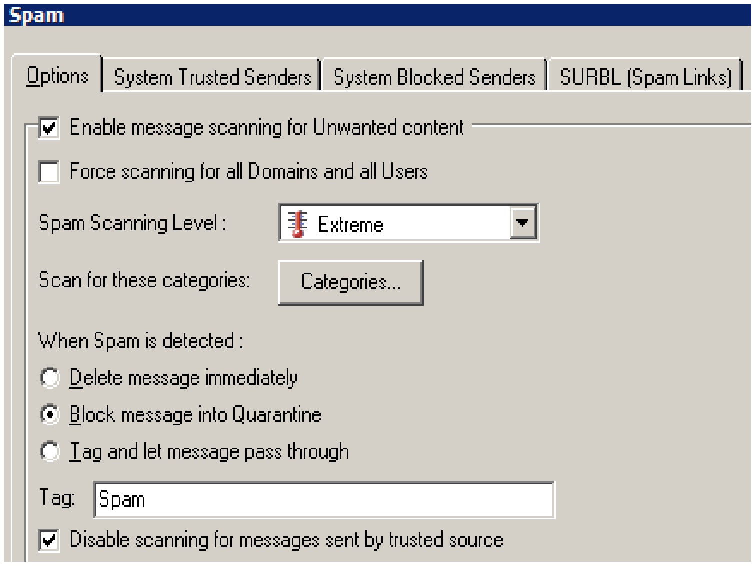
- Override cannot be selected if Force scanning for all Domains and all Users is checked in the system settings under Phishing.
- Configure your preferences for scanning level, message handling and whether this user can release phishing messages from Quarantine.

Spam

The Spam controls are separated into 2 layers of tabs: Properties and Preferences (seen at the bottom of the panel). This section begins with the Preference settings, which is where you set the scan levels and message handling rules.

Options

Use these settings to configure spam scanning for the entire system.



☑ Enable message scanning for Unwanted content

□ Force scanning for all Domains and all Users

Spam Scanning Level : Extreme

Scan for these categories:

When Spam is detected :

○ Delete message immediately

● Block message into Quarantine

○ Tag and let message pass through

Tag: Spam

☑ Disable scanning for messages sent by trusted source

Force scanning for all Domains and All users

- Overrides individual settings for users and domains and forces scanning on all messages.
- Do not use this function if you plan to allow domains and users override privileges.

Spam Scanning Level

- Select the level of aggressiveness for scanning: Disabled, Normal, Strong or Extreme.
- Extreme is set by default, but may produce False Positives. If this occurs, reducing it to Strong should provide a good balance between protection and little-to-no false positives.

Scan for these Categories

The Vircom spam filter categorizes messages based on their content. Click Categories to view the message types. Select which ones you want scanned, and uncheck those that should bypass the scan and be delivered.

When spam is detected

Select one of the following message handling options:

- Delete message immediately.
- Block message into quarantine.
- Tag and let message pass through:
  - Enter a tag or label to be added to the Subject line of a message (e.g. Spam).
  - This option is useful for those who prefer to receive all messages, but have their own filtering or rules mechanisms enabled in the mail client. The email rules can then determine what to do with messages based on the subject tag.

Disable scanning for messages sent by trusted source

- This function is used specifically for users who authenticate using SMTP Auth, to allow their outgoing mail to the Internet to bypass spam filtering (including the Vircom filter and custom scripts.)
- Incoming Internet mail will be scanned according to your settings.
- Attachment and virus scanning in the modusGate versions that support these functions will continue.

System Trusted Senders

“Trusted” senders are the people who are well known to you and whose email content you trust. These settings enable you to specify these known senders, allowing their mail to bypass spam scanning and be delivered.

Messages from trusted senders will continue to be scanned for viruses and forbidden attachments, however.

Enable Auto-Trusted List

Trusted Sender settings exist at the system, domain and user levels. These lists must be manually created and updated, which can be tedious and difficult to maintain.

The Auto-Trusted List instead provides an automated method for creating and maintaining the addresses, based on users' email behavior:

- When a person replies to an email that was originally sent from a local user (who has an account on your modusGate server), the responding address is automatically added to that **user's** Trusted Senders List.
- Auto-trusted addresses are not added to the System list.

To support the auto-trusted feature, the Default database configured for use with modusGate must be a SQL or SQL Express Server. (Access and PostgreSQL are not supported).

- To verify the Default database, go to System > System Databases > Default Database Settings.

Enable automatic cleanup of old records

This option applies only if the Auto-trusted feature is enabled.

- It automatically maintains the auto-trusted list to keep only the active addresses.
- Cleanup occurs once daily when a user's maximum limit has been reached.
- Addresses in the auto-trusted list are time stamped upon reply and the automatic cleanup feature deletes the data with oldest time stamps.
- Reoccurring addresses are time-stamped as they enter the database.
- There is a second automatic cleanup process whereby modusGate looks for mailboxes that have been deleted and removes all auto-trusted entries associated with them. This process occurs every 90 days and is not configurable in the Console.

Maximum number of auto-trusted addresses allowed per user

- Enter the maximum number of addresses permitted per user. The default is 1,000.

Additional information about the Auto-Trusted List

- It can only be configured at the system level.
- Is disabled by default.
- Auto-trusted addresses are added to each user's trusted senders list but are not visible to the users.

- Because auto-trusted entries cannot be viewed or edited, blocked senders lists take priority during scanning.
- An X-SCA-Stop header (X-SCA-Stop: [autotrust]) appears when a message is auto-trusted and is used by moduscan to display the sieve script execution results.
- When the maximum number of addresses is reached, the record with the oldest timestamp is removed.
- The mail server's IP address must be listed in the routing table in modusGate Console (see Connections).
- When recipients reply to messages sent from local users, the originating IP address will be compared to the routing table to establish 'trusted' local users and build their auto-trusted lists.

Enable System Trusted Senders List

Create a list of trusted domain names and email addresses that will bypass the custom Blocked Senders List, the Vircom filter engine and your custom sieve scripts. This is especially useful if you experience false-positives.

- Addresses in this list apply system-wide.

Click Add to enter addresses:

- Domain names and email addresses are supported.
- Wildcards are supported (e.g. *@domain.com).

System Blocked Senders

Blocked Senders are the addresses from which you never want to receive email.

Enable Blocked Senders List

Click to create a list of domains and email addresses that will always be blocked, regardless of the content.

Click Add to enter addresses:

- Domain names and email addresses are supported.
- Wildcards are supported (e.g. *@domain.com).
- It is possible to block an entire domain, but allow mail from a specific address in that same domain.

EXAMPLE Block all addresses from xyz.com by entering *@xyz.com to the Block List. Then add john@xyz.com to the Trusted Senders List.

When a message is received from a Blocked Sender

Select one of the following message handling options:

- Delete the message
- Send to quarantine
- Send to recipient with tag: Enter text to be added to subject line and the message will be delivered instead of blocked.

SURBL (Spam Links)

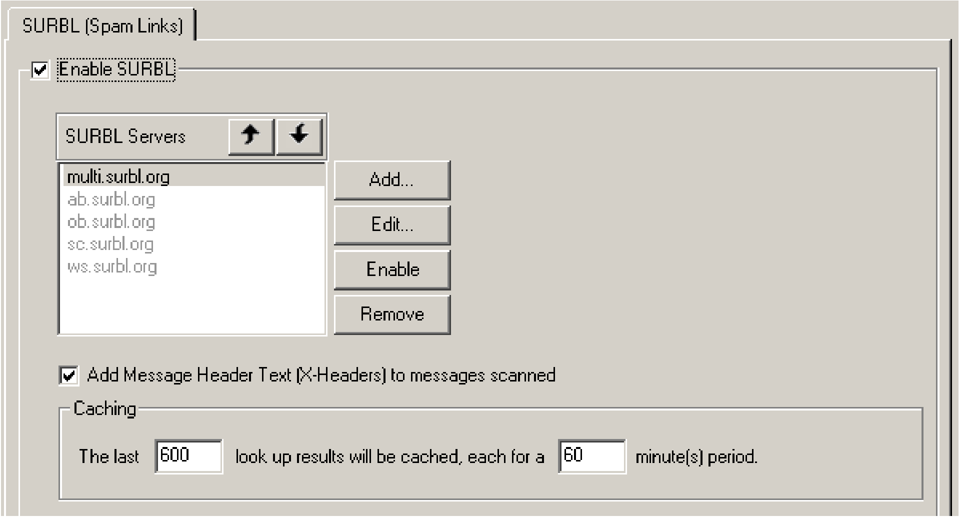
SURBLs differ from most other RBLs in that they are used to detect spam based on message body URLs (these are links - usually websites). Unlike most other RBLs, SURBLs are not used to identify spam **senders**. Instead, they allow you to identify messages that have spam hosts mentioned in the **message bodies**.

The lookup of email URLs is performed randomly, in case spammers bracket spam links in the list with legitimate links at either end of the list.

To use this feature:

Click Enable SURBL > select a server > click Enable > Apply.

You may optonally Add, Remove and Edit SURBL servers, and use the Up and Down arrow keys to move a server name in the list.



SURBL (Spam Links)

☑ Enable SURBL

SURBL Servers

multi.surbl.org
ab.surbl.org
ob.surbl.org
sc.surbl.org
ws.surbl.org

☑ Add Message Header Text (X-Headers) to messages scanned

Caching

The last 600 look up results will be cached, each for a 60 minute(s) period.

Add Message Header Text (X-Headers) to messages scanned

X-Headers can be added when a message matches a DNS **blacklist** entry and when it fails a validation test.

- These headers are used by the spam scanner.

- This function is enabled by default.

Caching

Configure how many lookup results will be cached and for how long.

Properties Settings

General

This panel provides update and version information for Vircom's proprietary spam filter, called Sequential Content Analyzer (SCA™).

- The spam definitions used by the SCA engine are updated automatically by Vircom and are not customizable.

Auto-Updates

The spam engine and its definition files are updated automatically by modusGate. It is set to look for new definitions every 15 minutes, which are applied automatically as they become available.

- You may optionally change this frequency.
- These updates only affect the filters that Vircom supplies. Any custom scripts you create will remain intact.

Auto-Cleanup

These settings allow you to specify when a message is deleted from the spam quarantine.

Messages are removed from both the quarantine folder and the database when the expiry date is reached, or when the maximum total size is reached - whichever comes first.

You may optionally modify these settings:

- Message expires after: enter the number of days.
- Max. Total Size: enter the number of KB.
- Start job at: enter a time using the format hh:mm.

Domain controls: Spam

Most spam scan preferences can be configured in the Domain properties in the console but there are some exceptions:

- Enabling Force scanning for all Domains and all Users in the System-level Spam settings will block the use of Domain overrides.
- Auto-trust sender settings are available at the System level only.
- SURBL settings are available at the System level only.

To configure Domain overrides:

Go to Domains > select domain name > Spam / Trusted Senders / Blocked Senders. Enable Override server default settings and configure your preferences.

NOTE The Domain-level Trusted Senders panel provides an additional option for Exchange Server users: Trust Exchange Users' Contact Lists.

This setting enables you to automatically trust the addresses that are stored in your users' Contacts and Safe Senders lists.

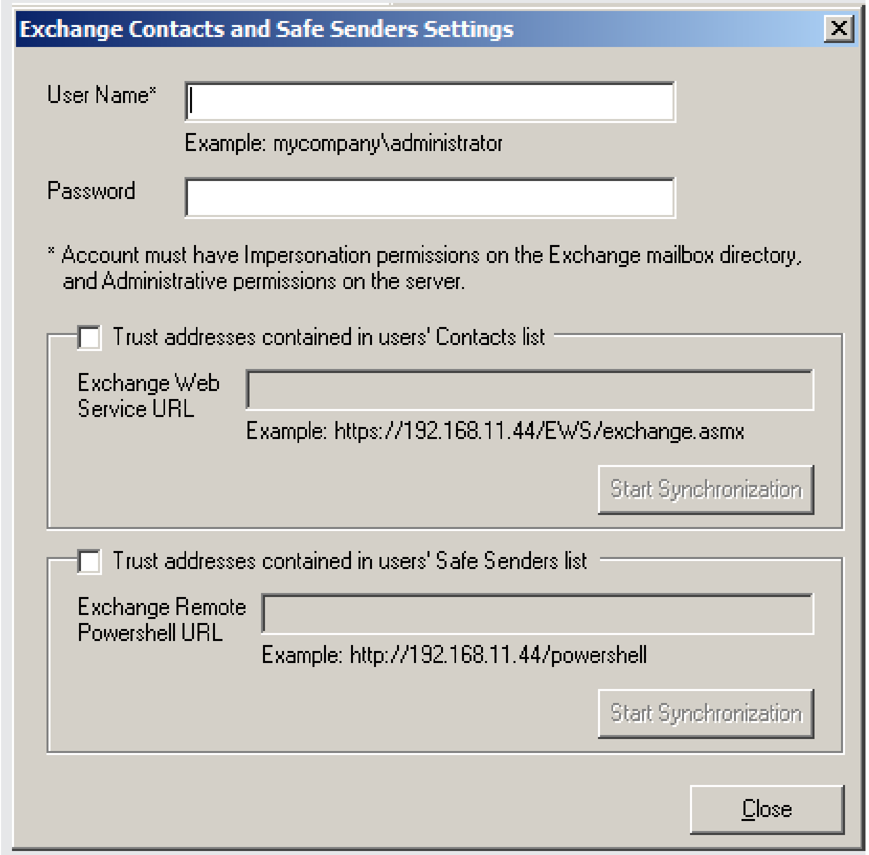
- Due to access restrictions in older Exchange versions, these features are only supported by Exchange 2007 and 2010, where indicated:
  - Auto-trust Contacts is supported for both Exchange 2007 and 2010.
  - Safe Senders Lists are supported for Exchange 2010 only.

Follow the instructions below to configure the settings:

Step	Action
1	Verify that modusGate's default database is set to use SQL/SQL Express Server (see System > System Databases > Default Database Settings.)
2	Configure Impersonation permissions for the account used to connect to Exchange: NOTE An Administrator account does not natively have Impersonation permissions. These are required to give modusGate remote access to the contents of the Contacts list.F
3	Log into the Exchange server with your Administrator account and load the Exchange Management Shell.

Step	Action

4	For Exchange 2007, run the following PowerShell command:
	`Get-MailboxDatabase | ForEach-Object {Add-ADPermission -Identity $_.DistinguishedName -User domain\administrator -ExtendedRights ms-Exch-EPI-May-Impersonate}`
	For Exchange 2010, run this PowerShell command:
	`New-ManagementRoleAssignment -Name:impersonationAssignmentName -Role:ApplicationImpersonation -User:domain\administrator`

5	In the modusGate console, go to: Domains > domain name > Trusted Senders > Trust Exchange Users' Contact Lists.  Exchange Contacts and Safe Senders Settings User Name* Example: mycompany\administrator Password * Account must have Impersonation permissions on the Exchange mailbox directory, and Administrative permissions on the server. ☐ Trust addresses contained in users' Contacts list Exchange Web Service URL Example: https://192.168.11.44/EWS/exchange.asmx Start Synchronization ☐ Trust addresses contained in users' Safe Senders list Exchange Remote Powershell URL Example: http://192.168.11.44/powershell Start Synchronization Close
6	Enter the Administrator's User Name and Password • The User Name must be in the format of domain\username.

Step	Action
7	Enable Trust addresses contained in users' Contacts list and enter the URL for the Exchange Web Service: EXAMPLE https://192.168.11.44/EWS/exchange.asmx • Option is available for both Exchange 2007 and 2010.
8	Enable Trust addresses contained in users' Safe Senders list and enter the URL for the Exchange Remote PowerShell: EXAMPLE http://192.168.11.44/powershell • Available for Exchange 2010 only.
9	Click Close to start the synchronization process automatically. Optional: The synchronization reoccurs automatically once per day, but you can use Start Synchronization to force a manual update.

Details of the synchronization process can be seen in the Operations (OPR) log, located in the ...\Vircom\modusGate\log directory.

NOTE Users cannot bypass the spam scanner by adding their own email addresses to their Contacts or Safe Senders lists.

User controls: Spam

To configure User overrides for spam settings:

Go to Users > select user name > Spam.

- Enable Override domain default settings and configure your preferences.
- Enabling Force scanning for all Domains and all Users in the System-level Spam settings will block the use of User overrides.

Trusted Senders and Blocked Senders also have user-level settings. Any addesses that users enter manually will be visible in these screens.

- If you had enabled the Auto-trust feature, those addresses will not be visible here. See **System Trusted Senders** for details.

Forbidden Attachments (F.A.)

You can block attachments by name or type which can help to prevent new types of viruses and unwanted content from entering your system.

The Forbidden Attachment controls are separated into 2 layers of tabs: Properties and Preferences (seen at the bottom of the panel). This section begins with the Properties settings, which is where you can configure the list of attachments to filter.

General

From this panel, you can set general properties for the attachment scanner.

Enable Smart File Type Detection (Fingerprinting)

- Used to enable Fingerprinting, a method by which the real attachment type of a specific file is detected.
- This 'catches' questionable attachments that have been renamed.

EXAMPLE update.doc has been renamed to update.txt. Fingerprinting will be able to detect that the file is actually a Word document.

Block zip files encrypted with a password

- Enabling this features ensures all zip files that have been password-protected are blocked from entering your mail system.

Automatically quarantine messages with attachments larger than

- When enabled, all messages with attachments larger than the specified size (in KB) will be quarantined.
- A value of "0" means that there is no limit.

Forbidden Attachments

This screen provides a ready-made list of attachments that will automatically be blocked by modusGate, such as *.BAT, *.EXE and other files that often carry viruses and other malware. However, the contents of this can be completely customized.

The files are grouped by severity (Normal, Strong and Extreme) to correspond to the filter aggression levels. Expand the groups to see the file names.

As with all other filters, the scan aggressiveness level for forbidden attachments can be adjusted at the system, domain and user levels.

However, the list of file attachments can only be configured in this system-level panel.

How to customize the list

Use Add to enter a new attachment type and to select the filter level.

- Wildcards are accepted in the names.

Import will import a list from a text file.

- Using Import will overwrite the current list.
- This file must contain text strings with wildcards, separated by a return.

Export will export the list to a text file.

Default will revert the entire list back to default content and levels.

Using the Edit button provides a number of options:

It can be used to change an existing file name and/or filter level, including the items in the supplied list.

EXAMPLE *.DLL files are under the Strong category, but can be moved to Normal by using Edit.

Being able to move files is especially useful if you want to set different scan levels for different people.

Scenario: you want to allow specific file types through for some users (Group A), but to block those files for all other users (Group B). Before making any changes, you need to know how the scan levels work:

- Extreme: ALL message types are blocked, including Extreme, Strong and Normal.
- Strong: messages in both the Strong and Normal groups are blocked.
- Normal: only the Normal group is blocked.

Returning to the scenario: to block file types for the majority of users (in Group B), place the files in either the Strong or Extreme category, and set the equivalent scan level for the Group B users. Because the users in Group A must recieve those files, set their scan level lower: to Normal.

Auto-Cleanup

These settings allow you to specify when forbidden attachments are deleted from the quarantine.

Messages are removed from both the quarantine folder and the database when the expiry date is reached, or when the maximum total size is reached - whichever comes first.

You may optionally modify these settings:

- Messages expire after: enter the number of days.
- Max. Total Size: enter the number of KB.

Postmaster

You can optionally notify the system Postmaster when a forbidden attachment is detected:

- Enter the name of the postmaster (default is Postmaster).
- Enter the email address for the postmaster account. This must be a valid account on the system.

Preference settings

Use the bottom tabs to access the Preference settings to configure the system-level scan controls.

Options

Set the scan level and message handling rules for the attachment-blocking engine.

Detect forbidden attachments within compressed files

- Scans compressed files for forbidden attachments.

Force scanning these Settings for all Domains and all Users

- Overrides the individual settings for users and domains and forces all users' mail to be scanned at the selected level.

Attachment Scanning Level

- Used to select the level of aggressiveness for attachment-scanning: Normal, Strong or Extreme.
- If Disabled is selected, attachment scanning is turned off.

Set the message handling options:

- Delete message immediately.
- Block message into Quarantine.
- Allow users to release quarantined attachments: use this option if there are issues with false positives, or if you want to allow users to release certain message types. Note that this option can also be set at the domain and user levels, to provide more control.

Alert Sender

This feature enables you to specify if and how to notify the sender that the message contained a forbidden attachment.

CAUTION Due to current behavior of spam and malware that spoof sender addresses, do NOT use this option. If enabled, false notifications are likely to be sent to people who did not actually send the attachment.

Alert Recipients

This feature allows you to specify if and how to notify the recipients when a message contains a blocked attachment.

NOTE Both directQuarantine and/or Quarantine Reports clearly label the messages that contain attachments, so you may want to use those features instead of the notification process.

Enable Alert Notifications to Recipients

- This must be turned on at the server level to be able to set individual controls at either the domain or user levels.

Recipients receive notification

- This server-level override function allows you to reset individual domains and/or users' settings to force everyone to receive alerts.
- Enter the Name, Address and Subject for the alert messages.

Select the message to be used for the alert:

- Use the default message.
- Use message from file: create a custom TXT or HTML file containing the notification text, and browse to select the file name.
- Use current message (plain text): enter your text in the window below.

Encoding

- Specify the text format: either Text / plain, or Text / HTML.
- Remember to enter the HTML code in the message body or specify an HTML file if you are pointing to a file.

Alert Substitutions

In the alert notifications, you may use two substitutions that will insert text based on the message being scanned and the results of the scan:

- Insert the sender name of the infected message: enter %1!s!
- Insert the scan report from the anti-virus engine: enter %2!s!

Domain controls: Attachments

Forbidden Attachment settings can be configured at the Domain level in the Console.

Go to Domains > select domain name > Attachments.

Enable Override server default settings:

- Override cannot be selected if Force scanning for all Domains and all Users is checked in the system settings under FA.
- Configure your preferences for scanning level, message handling and whether members of this domain can release attachments from Quarantine.
- The attachment list cannot be customized here.

User controls: Attachments

Forbidden Attachment settings can be configured at the User level in the Console.

Go to Users > select user name > Attachments.

Enable Override domain default settings:

- Override cannot be selected if Force scanning for all Domains and all Users is checked in the system settings under FA.
- Configure your preferences for scanning level, message handling and whether this user can release attachments from Quarantine.
- The attachment list cannot be customized here.

Rules

modusGate provides the ability to create custom scripts to better control spam in your environment. You can also use scripts to create message handling rules to meet compliancy regulations.

Language filters are also available to block foreign language spam.

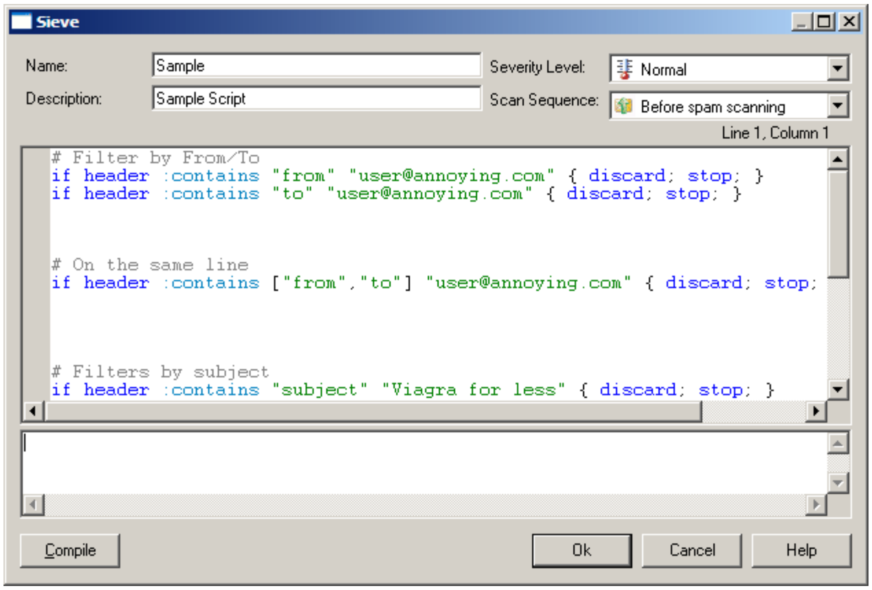
Custom Filter

From this panel, you can create custom sieve scripts for your system and place them in the order in which they should be executed.

NOTE Sieve is an email filtering script language that can be used with all operating systems and mail architectures. It is particularly useful for defining spam-filtering rules. Some script examples are given below, but for more examples, see the Knowledge Base article: http://kbase.vircom.com/kbase/default.asp?id=1333&SID=&Lang=1

Follow the instructions below to add or modify a sieve script:

Step	Action
1	Click Add to create a new script.



Name: Sample

Description: Sample Script

Severity Level: Normal

Scan Sequence: Before spam scanning

Line 1, Column 1

```
# Filter by From/To
if header :contains "from" "user@annoying.com" { discard; stop; }
if header :contains "to" "user@annoying.com" { discard; stop; }


# On the same line
if header :contains ["from","to"] "user@annoying.com" { discard; stop;


# Filters by subject
if header :contains "subject" "Viagra for less" { discard; stop; }
```

2	Enter the script Name and Description, where indicated.
3	Set the Security Level: Normal, Strong or Extreme.

Step	Action
4	Set the Scan Sequence: • Before all scanning: After security checks are passed, these rules have the highest priority and are run before ALL scan filters, including trusted and blocked sender lists, AND Virus and Attachment filters. – This option should therefore be used rarely and with caution. • Before spam scanning: (default setting). – Rules are applied after virus and attachment scanning but before any Trusted/Blocked sender lists and other filters are run. • After all scanning – These rules are applied last, after all other filters have run.
5	Type the text directly into the window or copy and paste existing text.
6	Click Compile to verify for syntax errors: • If there are no errors, No errors will appear • If there are errors, an error message will appear e.g. Line: 8, Column: 11 : Expected a quoted string or multi-line string NOTE Sieve scripts support UTF-8 characters. The scan engine treats the content according to the applied rules. Your spam severity settings will determine what levels of policy scripts are applied in the system.•
7	Click OK to exit the screen.
8	Enable the script. • Use Up or Down to change the priority of the script. • Scripts run in order: from top to bottom.
9	Use Disable to turn a script off. NOTE Restart the MODUSCAN service after deleting or disabling a script.

Enforcement of Corporate Email Policies and Parental Control

In order to customize sieve scripts effectively, modusGate employs an optimized receiving service to target mail traveling in specific directions. An attribute in the envelope of a message (.rcp file) identifies the message:

- Routing: From Outside to Outside
- Incoming: From Outside to Inside
- Local: From Inside to Inside
- Outgoing: From Inside to Outside

Trusted lists override the control script

- Unless trusted lists are disabled, some messages will bypass the control filter.
- If a client is using this feature for parental control, the Trusted Senders List on the child's PC must be disabled.
- Because processing order is important, the control script should be run last to avoid excess junk mail in the moderator's quarantine.

Corporate Control Scripts

The following provides examples of corporate control scripts. The moderator feature can be used as a parental control mechanism or a communications policy for companies, to forward messages to the moderator's quarantine mailbox for approval, while preserving header information.

```
if not envelope :matches "X-Sieve-Moderate" "*" {
                if header :contains "to" "suspiciousstaff@domain.com"
              {
                   if header :contains "subject" "job offers" {
                      x_moderate "moderator@mydomain.com";
         /* Send alert */
                      x_mailer "from@mydomain.com" "to@mydomain.com"
             text:
                         Subject: You have mail waiting for your
             approval
                         Please check your moderator’s QT.
             .
                         ;
                      stop;
      }
                }
}


if not envelope :matches "X-Sieve-Moderate" "*" {
               if envelope :contains "Local-Status" "outbound" {
                   if body :raw :contains "source code v1.0" {
                      x_moderate "moderator@mydomain.com";
         /* Send alert */
                      x_mailer "from@mydomain.com" "to@mydomain.com"
         text:
                 Subject: You have mail waiting for your
         approval
                 Please check your moderator’s QT.
         .
                 ;
               stop;
             }
           }
}
```

Explanation

When a message meets the filter criteria, it is quarantined to the account specified in the x_moderate line. This should be an account used solely for moderation purposes so that the messages are not lost among the other quarantined mail.

The alert portion of the script is optional. When a message is filtered, an alert notice can be sent to the second address in the x_mailer line (e.g. to@mydomain.com).

In the Administration Console's Quarantine, these messages will be tagged "[Requires Your Approval]" in the subject field. The WebQuarantine Quarantine view will display the subject specified in the script, e.g. "You have mail waiting for your approval."

The moderator is able to release the message and it will be delivered to the original recipient(s) with an additional header of "X-Sieve-Moderate".

Cascading Sieve Scripts

The sieve engine allows for multiple sieve scripts to be executed in cascading style. Therefore, the order in which your sieve scripts are listed in the Console is important.

Sieve script filtering for a given message ends because of three conditions:

- The message is rejected by the system, either through a reject, redirect or discard sieve command.
- A stop command is encountered in one of the scripts.
- The last sieve script in the list is executed completely.

Severity

The Severity of a sieve script corresponds to how drastic the filter is when blocking spam. There are three severity levels:

Normal: Will block less spam but ensure fewer false positives than scripts of higher severity.

Strong: Will stop more spam but may increase the risk of false positives.

Extreme: Ensures the capture of almost all spam within their category but may cause a larger number of false positives.

Categories

A script's category defines a script in more detail. Categories are numerous and can include such things as:

- phishing\viruses
- phishing\diet
- phishing\piracy

Levels of Severity

Scripts belonging to the same category but with different levels of severity are complementary. To receive full protection against spam in the phishing\viruses category, for instance, enable all three sieve scripts:

- phishing\viruses\normal
- phishing\viruses\strong
- phishing\viruses\extreme

Language Filter

The language filter can be set to block spam based on foreign languages and character sets.

This feature enables you to select which languages to block from a pre-set list. By default, all languages are allowed.

Message handling options include:

- Delete message immediately.
- Block message into Quarantine.
- Tag message with a subject message and allow it to pass through.

Select language content to block

- Click on » to add a language to the Blocked Languages list
- Click on « to remove language from the Blocked Languages list

Foreign Language Behavior

- Scanning for ▪ language content occurs:
  - After virus and attachment scanning
  - After the trusted and blocked lists
  - Before spam scanning by the SCA engine.
- Custom filters based on language content are supported; trusted addresses will bypass language filtering.
- Messages containing words or characters in several languages are given a language probability rating based on the weight of the content.
  - If the bulk of a message is in Italian, it will be considered ‘Italian’ and this is the code that will appear in the header envelope.
- The probability rating determines whether the message is filtered or not.
- If the bulk of the message is in a ‘permitted’ language but contains words or characters in blocked languages, the message will pass through.
- Messages considered spam are displayed in the ‘high spam probability’ section of the Quarantine Reports and can be released by the user.
- The header tag is accessible to sieve scripts and allows for the creation of custom rules based on language, such as exclusion rules.

The accuracy of language filtering depends upon the amount of text in the message body. A higher number of characters ensures better accuracy. Fewer than 256 characters in the message body could result in poor accuracy. This may occur if you have added Unrecognizable to the Blocked Languages list.

Performance

From this panel, you can set performance parameters to improve the performance of the spam engine.

Cache Size:

- Used to specify the number of entries to be kept in the performance cache.

- Presently, these options cannot be modified.

Reload Every:

- Used to specify how often modusGate™ verifies if there is a new script available and loads it into memory.
- Presently, these options cannot be modified.

Enable Attachment Size Verification

- Used to restrict scanning for large attachments (which can potentially slow system performance).

Do not scan messages with attachments larger than

- By default, the system will not scan messages if they contain attachments that are larger than 950KB.

Quarantine management

Overview of features

modusGate offers several methods for monitoring and controlling quarantined messages, for administrators and end-users alike.

1. The Quarantine panel in the Administration Console: gives the Administrator a global view of all users' blocked messages.

2. Quarantine Reports: summary reports that can be sent to users on a scheduled basis. See **Quarantine Reports** for configuration details.

3. WebQuarantine: a web application that users can log into to see a) their quarantined messages in realtime, and b) view and modify their filter settings, if allowed.

4. directQuarantine for Outlook: licensed separately but included with modusGate, this program allows users to view quarantined messages in realtime, using features built into Outlook, and to control the contents from there.

The following sections will decribe all these options.

Console administration

The quarantine panel in the Console allows you to monitor and view messages captured by the attachment, spam and anti-virus filter engines. Any addresses blocked by custom blacklists will also be included.

To capture all filtered messages system-wide, Block Message into Quarantine must first be enabled in each of the filter control panels: Virus, Spam, System Blocked Senders (within the Spam controls), Phishing and FA.

NOTE These same settings can also be configured at the Domain and User levels.

The panel is divided into 2 sections: the message Properties, and the Results.

The Results section displays a list of all of the quarantined messages, sorted and displayed separately according to the content:

- Spam displays messages blocked by the SCA, your custom sieve scripts and the custom blacklists.
- Attachments displays messages blocked by the Forbidden Attachment settings.
- Viruses displays the infected files.
- Phishing displays messages considered to contain phishing content.

A Find Result tab displays the search results for the Find command when searching for a particular message. See *"Find" on page 110*.

Using Quarantine Properties

Select a message in the Results list to view the message details in Properties:

Message: Shows the body of the quarantined message in the window, along with the From, To, Cc, Subject, Sent date and any attachments.

Headers: Shows the complete message header details.

Raw Source: Allows you to safely view the contents of a message to determine if it should be released (or not) without risk to your mail server.

Using Quarantine Results

Click on the tabs to browse messages in Spam, Attachments, Viruses and Phishing: each line in the Results window represents a blocked message.

Refresh

- Refreshes the list of messages in quarantine.
- When users delete items from their WebQuarantine, there is a slight delay before the value is registered in the Results window.

Release

- Releases messages from quarantine and delivers them to the intended recipient(s).
- Viruses cannot be released, by default, but the option can be enabled by making a change in the registry:
  - Open the Registry Editor
  - Go to: HKEY_LOCAL_MACHINE\SOFTWARE\Vircom\VOPMail
  - Create a new DWORD named ScanAllowedVirusesRelease
  - Assign one of the following values:
  - 0- (default): No virus can be released from quarantine
  - 1 - Only viruses identified as Possible virus can be released
  - 2 - All viruses can be released
  - If any other value is used, 0 will be assumed.

NOTE Allowing the virus release affects only the console and administrative actions: end-users are never allowed to release viruses.

Delete: Deletes messages from quarantine.

Mark as unread: Marks read quarantined messages as unread.

False-positive

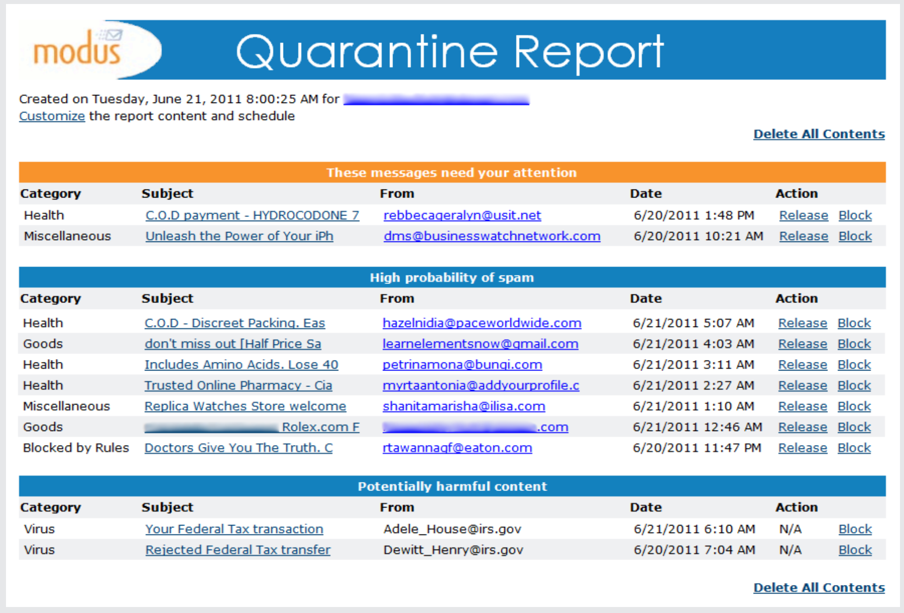
- Only for use with spam.
- A report is sent to Vircom identifying messages that you consider to be legitimate and improperly quarantined.
- Vircom's anti-spam team adjusts the filters to prevent future false-positives.

User administration

Quarantine Reports

The **Quarantine Reports** section described the configuration and scheduling of the reports; this section describes the report functionality.

When enabled, Quarantine Reports are emailed to users on a scheduled basis to provide a summary of their quarantine contents. The Reports can be configured to always show all quarantined messages, or to show only the new messages that have arrived since the last report was issued.



Quarantine Report

Created on Tuesday, June 21, 2011 8:00:25 AM for [redacted]
Customize the report content and schedule

Delete All Contents

These messages need your attention

Category	Subject	From	Date	Action
Health	C.O.D payment - HYDROCODONE 7	rebbecageralyn@usit.net	6/20/2011 1:48 PM	Release Block
Miscellaneous	Unleash the Power of Your iPh	dms@businesswatchnetwork.com	6/20/2011 10:21 AM	Release Block

High probability of spam

Category	Subject	From	Date	Action
Health	C.O.D - Discreet Packing. Eas	hazelnidia@paceworldwide.com	6/21/2011 5:07 AM	Release Block
Goods	don't miss out [Half Price Sa	learnelementsnow@gmail.com	6/21/2011 4:03 AM	Release Block
Health	Includes Amino Acids. Lose 40	petrinamona@bungi.com	6/21/2011 3:11 AM	Release Block
Health	Trusted Online Pharmacy - Cia	myrtaantonia@addyourprofile.c	6/21/2011 2:27 AM	Release Block
Miscellaneous	Replica Watches Store welcome	shanitamarisha@ilisa.com	6/21/2011 1:10 AM	Release Block
Goods	[redacted] Rolex.com F	[redacted].com	6/21/2011 12:46 AM	Release Block
Blocked by Rules	Doctors Give You The Truth. C	rtawannagf@eaton.com	6/20/2011 11:47 PM	Release Block

Potentially harmful content

Category	Subject	From	Date	Action
Virus	Your Federal Tax transaction	Adele_House@irs.gov	6/21/2011 6:10 AM	N/A Block
Virus	Rejected Federal Tax transfer	Dewitt_Henry@irs.gov	6/20/2011 7:04 AM	N/A Block

Delete All Contents

Report actions

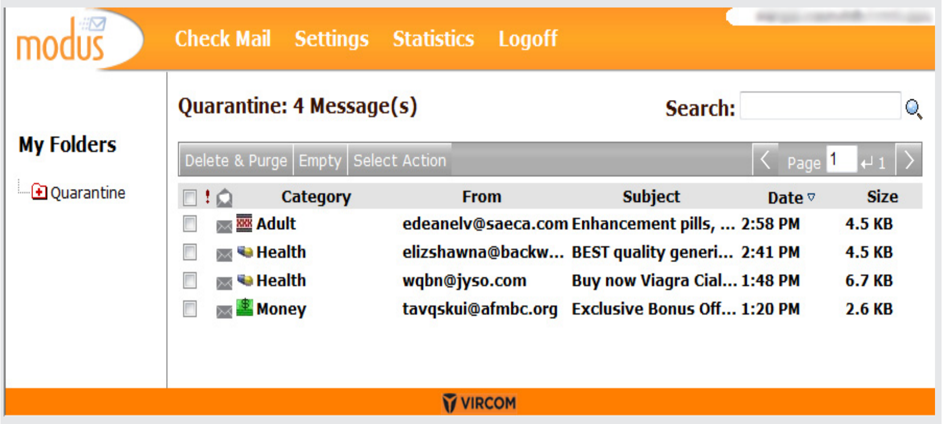
Reports allow users to perform the following functions:

- View the message content by clicking the Subject link: dangerous links within the message are inoperable or blocked.
- Release a message to the Inbox, when permitted (viruses can never be released)
- Additional release options include:
  - The ability to add the sender’s email address or domain name to his/her Trusted List
  - Ability to report the message as a false positive: a copy of the message is sent to Vircom so that adjustments can be made to the filters, if necessary.
- Block the message sender: the email address or domain name can be added to the Blocked List
- Delete all messages: deletes only the messages contained in the current report.
- Customize the report content and schedule: if enabled in the console, users can log into WebQuarantine to see their quarantine report content settings and schedule, and make adjustments.

WebQuarantine

This web-based application enables users to log in to see a live, updated view of their quarantined messages and to make adjustments to their settings, including: filter levels, quarantine report contents and schedule, and Trusted and Blocked Sender lists.

All report actions listed above are also available in the WebQuarantine.



Quarantine: 4 Message(s)

□	!	Category	From	Subject	Date ▽	Size
□		Adult	edeanelv@saeca.com	Enhancement pills, ...	2:58 PM	4.5 KB
□		Health	elizshawna@backw...	BEST quality generi...	2:41 PM	4.5 KB
□		Health	wqbn@jyso.com	Buy now Viagra Cial...	1:48 PM	6.7 KB
□		Money	tavqskui@afmbc.org	Exclusive Bonus Off...	1:20 PM	2.6 KB

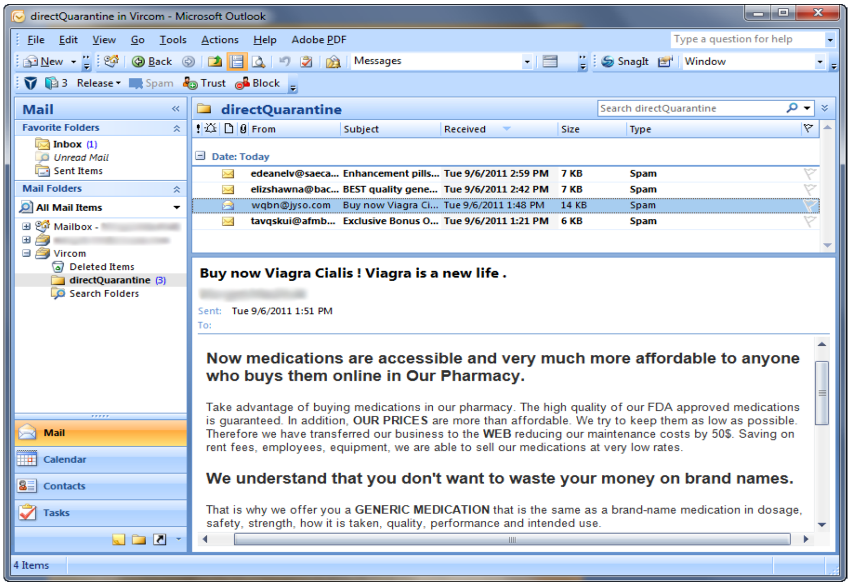
Users cannot change any of the filter settings or other controls without the administrator’s permission. Permission controls are located in the Console in Web > Privileges > Allowed User Properties. See *“Web” on page 107* for details.

A detailed description of this program and its functions can be found in the *WebQuarantine User Manual*, located in the …\Vircom\modusGate\Documentation folder.

directQuarantine for Outlook

This add-on program to modusGate provides users with a live, up-to-date view of their quarantined messages directly within Outlook.

Users are able to see the message type (spam, attachment, virus, etc.), and can perform release, delete, block and trust functions, using buttons embedded in Outlook's toolbar/ribbon controls. In addition, users have the added ability to report messages as spam, if and when they slip by the filters.



From	Subject	Received	Size	Type
Date: Today				
edeanelv@saeca...	Enhancement pills...	Tue 9/6/2011 2:59 PM	7 KB	Spam
elizshawna@bac...	BEST quality gene...	Tue 9/6/2011 2:42 PM	7 KB	Spam
wqbn@jyso.com	Buy now Viagra Ci...	Tue 9/6/2011 1:48 PM	14 KB	Spam
tavqskui@afmb...	Exclusive Bonus O...	Tue 9/6/2011 1:21 PM	6 KB	Spam

Buy now Viagra Cialis ! Viagra is a new life .

[redacted]

Sent: Tue 9/6/2011 1:51 PM

To:

Now medications are accessible and very much more affordable to anyone who buys them online in Our Pharmacy.

Take advantage of buying medications in our pharmacy. The high quality of our FDA approved medications is guaranteed. In addition, **OUR PRICES** are more than affordable. We try to keep them as low as possible. Therefore we have transferred our business to the **WEB** reducing our maintenance costs by 50$. Saving on rent fees, employees, equipment, we are able to sell our medications at very low rates.

We understand that you don't want to waste your money on brand names.

That is why we offer you a **GENERIC MEDICATION** that is the same as a brand-name medication in dosage, safety, strength, how it is taken, quality, performance and intended use.

The directQuarantine Server application is installed automatically with modusGate. It is available for use as a 30-day trial and for licensed users.

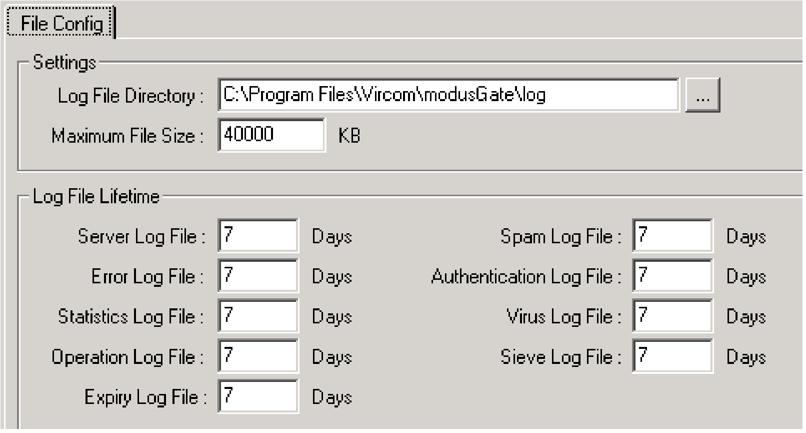
The Client application must be installed and configured separately as a Group Policy Object (GPO) on your Active Directory Server. To access the directQuarantine Client installation program and other files, go to Start > Programs > Vircom > dQ.

A detailed description of the Client installation, configuration and user interface can be found in the *dQ AdminGuide,* located in the …\Vircom\modusGate\Documentation folder.

Logs

File Config

This tab contains the core settings for the modusGate log files: where the files are stored, limits for controlling the log size and for determining how long they are kept.



File Config

Settings

Log File Directory : C:\Program Files\Vircom\modusGate\log

Maximum File Size : 40000 KB

Log File Lifetime

Server Log File :	7	Days	Spam Log File :	7	Days
Error Log File :	7	Days	Authentication Log File :	7	Days
Statistics Log File :	7	Days	Virus Log File :	7	Days
Operation Log File :	7	Days	Sieve Log File :	7	Days
Expiry Log File :	7	Days			

Logs are text files that can be stored anywhere within your network, including a shared drive. To change the location, enter the full path in Log File Directory, click Apply, and stop/restart all modusGate services to register the change.

The naming format for the files is TTTyyyymmdd.LOG, where:

- TTT represents a log type, e.g. OPR (Operation log), ERR (Error log), etc.
- yyyy represents the four digits of the year.
- mm represents the month, expressed as a number from 1 to 12.
- dd represents the day of the month.
- When a log reaches its maximum size, it is renamed with an appended number, e.g. OPRyyyymmdd-1.log, and a new ‘active’ log begins. The active log is the one without an appended number. The older logs are numbered sequentially.

Maximum File Size: the default size ensures that the log can easily be opened with Notepad or another text editor. If you change the size, simply click Apply - there is no need to stop any services.

Log File Lifetime: Enter the number of days a particular log file will be stored on the server.

- At the end of the life span, the files are deleted.
- If the value is set to 0, the files are never deleted.

Below is a summary of the options for each of the log types:

Log Name	Event Description
Statistics	Logs the following counters: SMTPRS • SMTPRS-NB_CONNECTION – Records the total number of connections to the SMTPRS service for all logins • SMTPRS-NB_RECEIVED_MSG – Records the total number of messages received by the service. • SMTPRS-NB_SERVICE_START – Records the total number of times the service has been restarted. SMTPDS • SMTPDS-NB_MSG_SENT – Records the total number of messages that have been sent by the service. • SMTPDS-NB_LOCAL_DELIVERY – Records the total number of messages that have been delivered to local domains and mailboxes by the service. • SMTPDS-NB_SERVICE_START – Records the total number of times the service has been restarted.
Server	Services Start and Stop: An entry is made whenever a service is started or stopped. Retry Domain(s): An entry is made whenever SMTPDS is instructed to immediately retry the pending domains. Change Configuration: This item is not recorded. The above items can also be logged in the Windows Event Viewer.

Log Name	Event Description
OPERATION	Protocol Exchanges: Logs every SMTP command sent to and response received by the system. Extended Protocol Exchanges: Logs every extended protocol command sent and response received by the system. Received Message Data: All message data received by SMTPRS is logged in the operation log file. • This information creates huge log files and should be used for debugging purposes only • At no time should you enable this feature for every-day use Transmitted Message Data: All the message data sent by SMTPDS is logged in the operation log file. • This information creates huge log files and should be used for debugging purposes only • At no time should you enable this feature for every-day use Received Transaction Summary:A summary of message receipt is logged. It can also be logged in Windows Event Viewer. Transmitted Transaction Summary: A summary of the message transmission is logged. It can also be logged in Windows Event Viewer. Network Connections: Incoming and outgoing network connections are logged. DNS Transactions: DNS requests sent by modusGate and the responses received are logged in the operation log file. • This information creates huge log files and should be used for debugging purposes only. • At no time should you enable this feature for everyday use. Dialup Connections: Not applicable to modusGate. Scanning Operations: Logs all operations of the scanning engine.

Log Name	Event Description
ERROR	Protocol Command Failures: SMTP failed commands sent and responses received are logged. Authentication Failures: Failed authentication attempts using SMTP AUTH server are logged. Network I/O Failures: Failed network I/O operations are logged. File I/O Failure: Failed file I/O operations are logged. DNS Failures: Failed DNS operations are logged. General Errors: Other failure types are logged. Scanning Errors: All errors involving the MODUSCAN engine are logged. All items can also be logged in the Windows Event Viewer.
SECURITY	This information ties in with the features found in the Security panel (see *“Security” on page 47*) Reverse DNS: Messages rejected due to a failed DNS Lookup. RBL: Messages rejected after RBL Lookup. Anti-Bulk: Messages rejected because of the Block Scan Attack feature. Relay: Messages rejected because of anti-relaying protection. MX: Messages rejected for not having a valid associated MX record. Protocol filter: Messages rejected by the protocol filter. Reject Address: Messages rejected because their address was blocked. Reject Host: Messages rejected because the host was banned. Banned IP: Messages rejected because the originating IP was banned. SPF: Results of the SPF lookups. SURBL: Messages rejected because of SURBL lookups.

Log Name	Event Description
AUTH.	Logs configured from this panel pertain to end-user logins to the web applications. Valid Login: Logs all valid logins. Invalid Login: Logs all invalid logins.
VIRUS	Detected viruses: Logs information about messages containing viruses and the name of the virus.
SPAM	Discarded messages: Logs information about messages filtered by the scan engine.
MESSAGE AUDIT	System-wide: Enables Audit logging for the entire system. Log expires in: Specify when the log will expire (in days). Enable Audit Log Auto Shutdown: Temporarily stops auditing in the event of a high load on the server or a database failure. • When the audit log is shutdown, new messages will not be audited until the load decreases or the database problem is resolved. • Messages received immediately before the shutdown will be audited but may not be found in the database. Set Audit Content: Click to select which of the following audit events to log: • Select Logging Template: – Full Logging logs all results – Basic Logging logs the most common results – Custom Logging appears when you manually select the events to log. • Select Scan Results to be Logged: Displays the selected filtering results. • Select Status to be Logged: Displays the selected message processing status. Information is updated dynamically as messages progress through the system and/or are filtered. CAUTION This log is processor intensive. To reduce the load on the system, consider doing the following: • Limit the number of events to log. • Enable Audit logging for specific domains or users: override settings exist at both the Domain and User levels.

Web

WebAdmin Privileges

This section is subdivided into 2 sets of properties: WebAdmin and Quarantine (see the lower-level tabs).

Beginning with WebAdmin, this panel contains the privileges (or permissions) settings that are used by both the WebAdmin and WebQuarantine applications. These privileges determine what settings users can or cannot change themselves.

Allowed Domain properties: Specify the domain-level settings that an administrator can modify using the WebAdmin console. All options except Message Audit and Domain Keys are enabled by default:

:

- Reporting
- Virus Levels
- Virus Actions
- Virus Alerts
- Phishing Levels
- Phishing Actions
- Attachment Levels
- Attachment Actions
- Attachment Alerts
- Spam Levels
- Spam Actions
- Trusted Senders
- Blocked Senders
- Blocked Senders Actions
- Blocked Senders Max. Size
- Message Audit
- Domain Keys

Allowed User properties: There are two sets of privilege levels for this feature that affect both the WebAdmin and WebQuarantine applications.

- Administrators (i.e. System and/or Domain Administrators): These settings determine the user-level properties that administrators can modify using the WebAdmin program.
  - All properties listed below are enabled by default, except Message Audit.
- Normal Users: These settings determine what users can modify using the WebQuarantine program.
  - Users do not have access to Message Audit.

- Reporting Frequency
- Reporting Content
- Generate Reports
- Virus Levels
- Attachment Alerts
- Spam Levels
- Spam Actions
- Language Filter

- Virus Actions
- Virus Alerts
- Phishing Levels
- Phishing Actions
- Attachment Levels
- Attachment Actions
- Language Filter Actions
- Trusted Senders
- Blocked Senders
- Blocked Senders Actions
- Aliases
- Message Audit (Admin list only)

Reset overriding for all Domains: Click to reset all domain-specific overrides to the default system-wide settings. This removes all domain overrides from the Domains panel.

Allowed User types: This feature is available but not required because users are created automatically in modusGate.

Domain controls: WebAdmin

If you have multiple domains, you can set different WebAdmin privileges per domain, as described above.

The Administrators section enables you to specify which users will have access to the WebAdmin panel to act as domain administrators.

Click Add to select the users who will have administrator rights. These users will be able to modify domain and user settings as defined above.

User controls: WebAdmin

From this panel, you can specify which users will have access to the WebAdmin panel to act as domain administrators.

Click Add to select the users who will have administrator rights. These users will be able to modify settings for all users as defined above.

Quarantine options

Web users directory: Specifies the directory where users' quarantined messages and custom settings are stored (including changes to filter options, quarantine report contents and schedule settings, and statistics regarding the number and type of filtered messages).

WebAdmin URL: By entering the WebAdmin URL in this field, WebQuarantine and WebAdmin work in conjunction with each other.

EXAMPLE WebAdminURL = http://localhost/WebAdmin/•

- The URL must always end with a forward slash '/'
- In WebQuarantine, when users click on **Settings**, they will be logged on automatically to WebAdmin to configure their mailbox settings.

IP List for Web Servers Authentication: Can be used to specify IPs that have access to the web applications.

- This is not generally used if modusGate is configured to do internal routing to a single Exchange / mail server.

Quarantine advanced

Encoding: Used to specify the default character encoding for WebQuarantine.

- If using Latin characters, keep the default setting, US-ASCII.

Visual settings: Used to specify the number of contacts and messages that appear on each page in WebQuarantine.

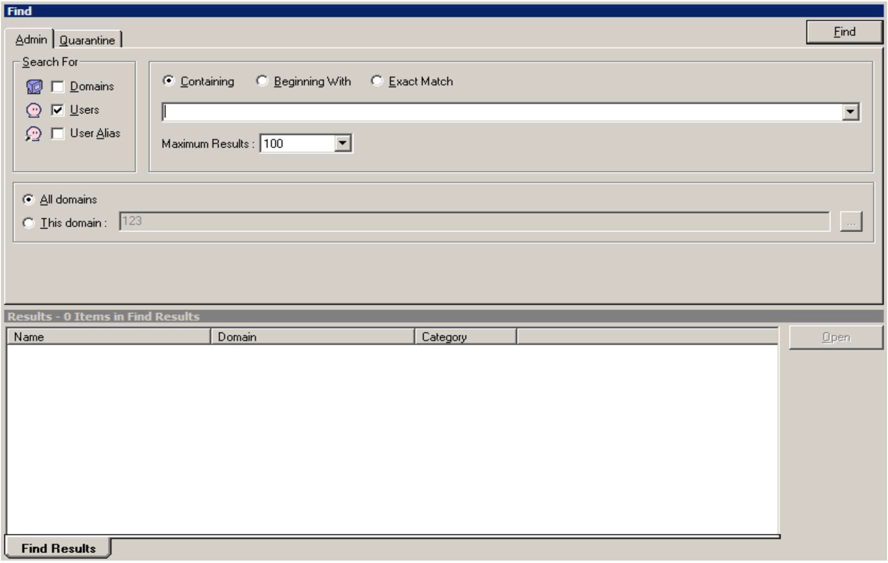
- If there are too many contacts or messages to be displayed on one page, page numbers become available, allowing you to scroll through all pages.

Find

With this feature, you can easily search for users, domains and quarantined messages (where applicable). This feature is convenient if you have multiple domains or a large user base.

Admin

Follow the instructions below to use the Find feature:

Step	Action
1	In Search For select Domains, Users, and/or User Alias. 
2	Select Containing, Beginning With or Exact Match and enter the text to search. Wildcards (*) can be used.
3	Maximum Results: set the number of results to display in the Find Results window.
4	Select to search All Domains or This Domain and enter the name. You can optionally browse the domain list using the ellipsis button (...) The latter function is navailable if multiple Search For items are checked.
5	Click Find to display the results in the Find Results window. Double-clicking an item in the results list will open its properties page.

☐ Domains
☑ Users
☐ User Alias

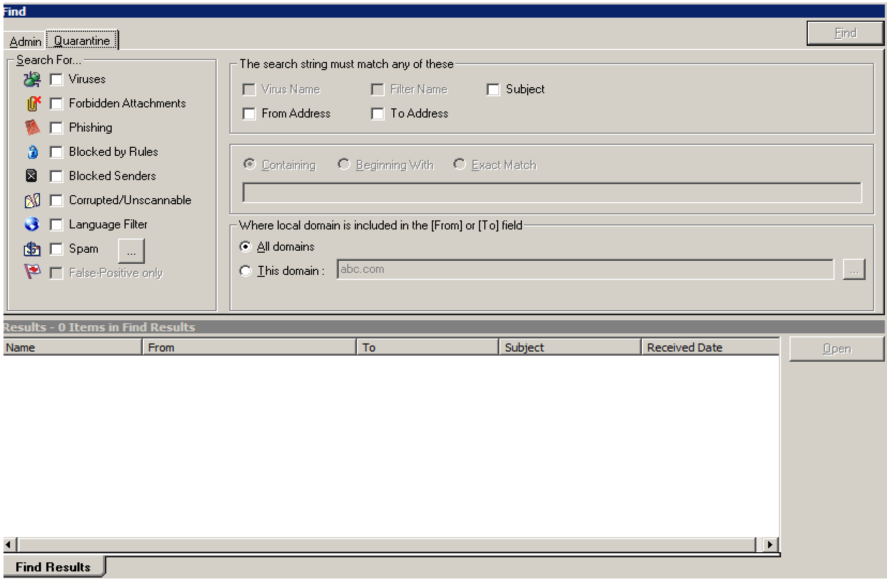
● Containing ○ Beginning With ○ Exact Match

Maximum Results : 100

● All domains
○ This domain : 123

Quarantine

This feature allows you to search for specific messages in the Quarantine.

Step	Action
1	In Search For select one or multiple filter types. When Spam is selected, you can further specify a message category by clicking the ellipsis button (...).  Find Admin Quarantine Find Search For... □ Viruses □ Forbidden Attachments □ Phishing □ Blocked by Rules □ Blocked Senders □ Corrupted/Unscannable □ Language Filter □ Spam ... □ False-Positive only The search string must match any of these □ Virus Name □ Filter Name □ Subject □ From Address □ To Address ● Containing ○ Beginning With ○ Exact Match Where local domain is included in the [From] or [To] field ● All domains ○ This domain : abc.com ... Results - 0 Items in Find Results Name From To Subject Received Date Open Find Results
2	Select which search string(s) to match.
3	Select Containing, Beginning With or Exact Match and enter the text to search. Wildcards (*) can be used.
4	Select to search All Domains or This Domain and enter the name. You can optionally browse the domain list using the ellipsis button (...)
5	Click Find to display the results in the Find Results window. Double-clicking an item in the results list will open the Quarantine panel to display the properties of the selected message. The same Find Results will also be displayed in the Quarantine > Find Results tab.

Section 5

Troubleshooting

Troubleshooting

This section provides help for the more common issues you may encounter with modusGate. Vircom also maintains detailed information on its Knowledge Base site at:

http://kb.vircom.com/Kbase

Connection problems with Exchange/AD

Problem: modusGate does not seem to be able to connect to Active Directory. Or, when another LDAP Browser is used, a connection still cannot be made.

Resolution: There may be a network problem such as a firewall or network translator not set up properly. To quickly rule out these problems is to telnet from the modusGate machine to the AD Port (389 or 3268). If something is preventing the connection, the following error will appear:

"Connecting To 192.168.0.112...Could not open a connection to host on port 389: Connect failed"

Problem: The Exchange Server and modusGate are not working properly when installed on the same PC.

Resolution: Open the Exchange System Manager. Go to Servers> ComputerName > Protocols > SMTP > SMTP Virtual Server. Right-click on SMTP Virtual Server > Properties. Make sure the All unassigned is selected in the list box and that the port number is changed to something other than Port 25 under the Advanced tab.

If you absolutely need to define an IP address, enter the IP address that is specified in modusGate's Connection panel in the Console when you are configuring the connection. Otherwise, the Exchange service will not be reachable.

Problem: Is my Domain Controller using the Global Catalog?

Resolution: On your Active Directory Domain Controller, click on Start > Programs > Administrative Tools > Active Directory Sites and Services

- Expand the site name (by default this will be called "default-first-site-name")
- Expand the Servers folder
- Expand the server to be verified
- Named vs. Default
- Right-click on NTDS Settings and select Properties

- Check whether the Global Catalog checkbox is enabled

Problem: Aliases from other domains are not working or cause unwanted results.

Resolution: modusGate supports alias aggregation across multiple domains (i.e. cross-domain alias support). modusGate considers the primary SMTP address* as the mailbox. The domain specified in the primary address will be the only mailbox listed in modusGate. All subsequent entries, regardless of the domain, will be specified as aliases in the user's alias list in modusGate. This keeps mailbox counts accurate and on par with Exchange Server and further consolidates all spam messages into a single quarantine.

If the primary address is specified as an internal Active Directory domain (e.g.: *.local*), you must either specify your primary SMTP email domain as primary or add an entry for that domain address in the modusGate Connections panel in the Console.

*The SMTP address information can be found in the Active Directory Users and Computers MMC as well as the Recipient policy in the Exchange Service Manager.

Mail delivery problems

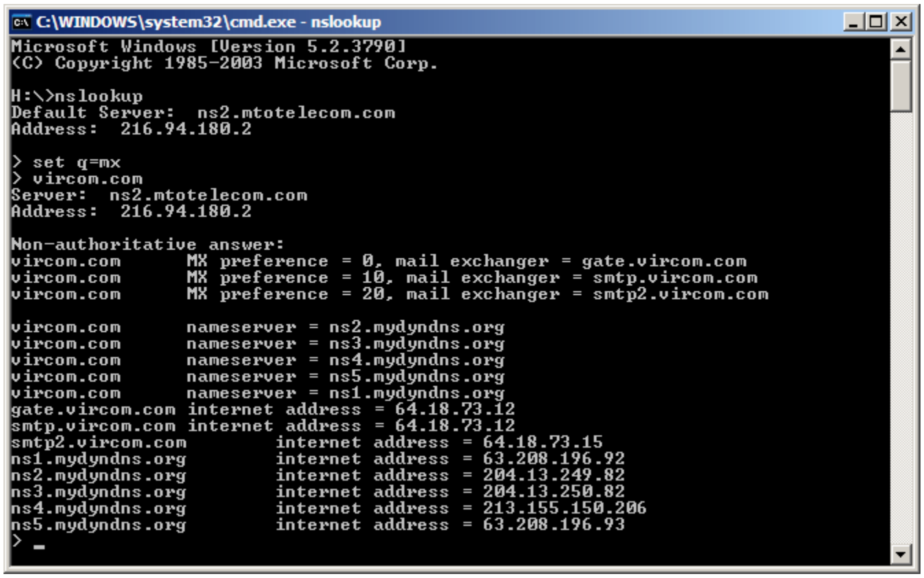
If modusGate is unable to send outbound mail to the Internet, use the following information to try to resolve the problem:

1. To rule out an invalid DNS setting, perform an nslookup of the domain to which users are attempting to send mail:

EXAMPLE resolve vircom.com

- At a command prompt, type: nslookup <enter>
- At >, type: set q=mx <enter> to query the MX record

- At > type: vircom.com <enter>



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

H:\>nslookup
Default Server:  ns2.mtotelecom.com
Address:  216.94.180.2

> set q=mx
> vircom.com
Server:  ns2.mtotelecom.com
Address:  216.94.180.2

Non-authoritative answer:
vircom.com      MX preference = 0, mail exchanger = gate.vircom.com
vircom.com      MX preference = 10, mail exchanger = smtp.vircom.com
vircom.com      MX preference = 20, mail exchanger = smtp2.vircom.com

vircom.com      nameserver = ns2.mydyndns.org
vircom.com      nameserver = ns3.mydyndns.org
vircom.com      nameserver = ns4.mydyndns.org
vircom.com      nameserver = ns5.mydyndns.org
vircom.com      nameserver = ns1.mydyndns.org
gate.vircom.com internet address = 64.18.73.12
smtp.vircom.com internet address = 64.18.73.12
smtp2.vircom.com        internet address = 64.18.73.15
ns1.mydyndns.org        internet address = 63.208.196.92
ns2.mydyndns.org        internet address = 204.13.249.82
ns3.mydyndns.org        internet address = 204.13.250.82
ns4.mydyndns.org        internet address = 213.155.150.206
ns5.mydyndns.org        internet address = 63.208.196.93
> _
```

The results show that mail goes to gate.vircom.com (pref level 0) and, if gate.vircom.com is down, mail is redirected to smtp.vircom.com (pref level 10).

2. If the DNS server still has problems when resolving names, perform a lookup using an external DNS server (in this case, Vircom's) to verify if your domain can resolve outside DNS servers.

- At a command prompt, type nslookup 64.254.224.2 <enter>

- If DNS is properly configured, there could be a network connection problem.

- The mail firewall could cause problems:

  - By default, some firewalls, such as Cisco Pix, block the extended SMTP commands required when using SMTP_VRFY or SMTP AUTH connection methods.

3. If the problems appear to be caused by DNS timeouts, two Registry keys can be added to automatically handle the failure. To change the default values, these keys must be created manually. The settings are used by SMTPRS, SMTPDS and MODUSCAN.

The new DWORD Registry keys must be created under HKEY_LOCAL_MACHINE\ Software \ Vircom \ Vopmail.

- DNSFailTimeout

  - This controls how long to wait (in seconds) before trying the secondary DNS when the primary is down
  - The default value is 30 mins

- DNSRetryTimeout
  - This controls how long (in seconds) to retry the primary DNS server when using the secondary
  - The default value is 1 day

NOTE You must restart the SMTPRS, SMTPDS and MODUSCAN services after creating the new key.

Mail Spool Directories

The message Spool (or queue) contains the message files as they are being processed by modusGate. The directory is located in ...Vircom\modusGate\Spool, and contains the following subdirectories:

Invirus

- Contains all messages waiting to be scanned (e.g. virus and spam).
- Messages found to contain unwanted content are sent to the Virus or Spam subdirectory, accordingly.
  - Messages containing viruses and spam are then sent to the Mailboxes\@Quarantine\Inbox folder (to provide a view of the content to Quarantine Reports, WebQuarantine and directQuarantine).
  - The message headers are written to the quarantine database.
- If none of modusGate's filters detect suspect content, the message is sent to the Incoming directory to begin the delivery process.

Incoming

- In modusGate L, where Invirus does not exist, this directory holds messages received by the SMTP receiver.
- In all other versions, it receives messages that have first undergone scanning.
- The SMTP Delivery Agent also places messages here, such as non-delivery reports.

Holding

The SMTP Delivery Agent moves messages from the Incoming directory into this directory when attempting to deliver the messages.

Domains

- When a message is moved into the Holding directory, the Delivery Agent creates a subdirectory within the domains directory for each domain to which a message is addressed (e.g. gmail.com, yahoo.com, etc.)
- If the message is for a local user, it creates a subdirectory called $local$
- Each subdirectory stores routing information and information about the message recipients on that domain
- The message itself stays in the holding directory until it can be sent to the destination address

Dead

- This directory stores messages addressed to the Postmaster but which cannot be delivered.
- It also collects messages that have caused a mail loop.
- A text file describing the reason for their 'death' is provided with the messages.

Diagnosing problems using spool directory contents

After mail passes through the security checks, modusGate processes the messages according to the configured scan settings and follows your quarantine rules.

Resolving an Invirus backlog

In Windows Explorer, go to ...\Vircom\modusGate\Spool\Invirus to verify if there is a backlog of .MSG and .RCP files.

Use the Refresh function to verify if the messages are flowing through the Invirus directory in a timely manner.

A backlog with the MODUSCAN engine can be caused by the following:

- Quarantine is slow or corrupt
- There could be a backlog of messages in ...\spool\spam or ...\spool\virus

- Using MS Access for the Quarantine database could cause a problem
  - MS Access has a size limitation of 2GB and, if the database nears 2GB, the MODUSCAN service will spike to 100% CPU
  - Consider using SQL Server or SQL Server Express for the Quarantine database
- If you choose to continue using MS Access, you may need to replace your database
  - Go to ...\Vircom\modusGate\mailbox\@quarantine
  - If the mailstore.mdb file is at or close to 2GB you must:
  - In the Console, go to System > Services
  - Stop the MODUSADM service
  - In Windows Explorer, go to the ...mailbox\@Quarantine folder
  - Rename the mailstore.mdb file to mailstore.old (a new one will be recreated)
  - Rename the ...@Quarantine\inbox folder to ...\Quarantine\inbox.old
  - In Services, start the MODUSADM service
  - modusGate should start processing the backlog

CAUTION The problem will likely occur again if you continue using an MS Access database

- Using an SQL Server or SQL Server Express database is recommended
- In the interim, if users consent, a work-around is to delete spam instead of sending it to Quarantine
- In the Console, go to Spam > Preferences > Options
- Select Delete the message immediately

Sieve script mistakenly capturing test messages

If test messages are being captured and sent to Quarantine, check that your custom sieve scripts are set up properly.

NOTE Do not set your Quarantine to Delete Spam when testing custom sieve scripts. This setting will not effectively determine if the sieve scripts are causing problems.

Third-Party anti-virus blocks messages and locks files

Some customers run third-party anti-virus software on the same machine as modusGate. This can cause problems on modusGate versions that provide scanning because the other AV program often locks files as modusGate attempts to scan them, interfering with message processing.

To avoid this situation, ensure that your third-party anti-virus package does not scan the following folders and their sub-folders:

- ...\modusGate\Spool
- ...\modusGate\mailbox\@quarantine
- c:\winnt\temp

Resolving backlogs in Holding and Domains folders

The ...\modusGate\spool\holding folder stores messages bound for local and outbound delivery. If there are more than 2,000 messages in this folder, there may be a problem. However, the content of the ...\modusGate\spool\domains folder is more important as this is what modusGate uses to coordinate mail delivery.

- Check local deliveries:
- Go to the ...\spool\domains\$local$ folder to verify the contents
- If there is a large backlog of messages, something is preventing the processing of messages going to the local domains
- In the folder, there should be one of four types of files which are of the same type (envelope files) but the extension of the files indicates what processing has been completed
- .RCO files: recently arrived .RCP files that have yet been scheduled for delivery
- .RCP files: scheduled for delivery and awaiting processing
- .LCK files: locked .RCP files that are in the process of being delivered
- .DEF files: deferred files have undergone a delivery attempt and are awaiting retry
- In the Console, go to System > Mail Delivery and click Deliver Now
- In the ...\spool\domains\$local$ folder, press *<F5>* to refresh the contents of the folder
- If the number of files does not decrease or if it increases after performing a Deliver Now, this signifies a problem
- The backlog might be due to communication problems with the authentication server

Possible causes for the backlog

- Authentication failing for local domains

- If your authentication server (AD or LDAP) is down or stops responding, delivery to local mailboxes will fail
  - On the modusGate server, open a telnet session to the mail server to check if it responds to Port 25
  - In the telnet session, open a connection to the modusGate server on Port 25 and try to send a message to a valid user
  - If the authentication server is unavailable, an error message will appear stating that there is a problem with your user authentication
- Contact Customer Support at support@vircom.com

Invirus Buildup and/or Server Freezes at Regular Intervals

Symptom:

Server seems to freeze at regular intervals making the machine unresponsive for short periods of time (less than a few seconds). In extreme cases, this can cause spool backlogs.

Cause:

modusGate updates information in the Registry. These write-operations to the Registry are cached in a file called software.log. By default, the OS will purge the cache and write the operations to the Registry hive every 5 seconds for Windows Server 2003 or every 5 minutes Windows 2000 Server.

During these intervals, the system appears to freeze. This behavior is not normal. The root cause is usually a poorly configured RAID controller whereby the Windows operating system is installed with a RAID array.

Solution:

If you use a RAID array for your OS drive with the RAID mode set to **write-through mode** instead of **writeback mode**, by default, the controller only sends an acknowledgement of a disk-write operation **after** the disk-write has completed. In the example above, no disk-write operations would be acknowledged until the RAID controller has finished purging the cache file and has merged it into the Registry hive. Therefore, it is recommended that the RAID controller on the OS drive be set to use **writeback mode** which sends an acknowledgement before the write-operation is complete. This ensures faster response.

For additional information, please consult the IBM Systems Software Information Center article **Understanding write-cache mode for logical drives**.

Web Application Issues

If the Web components are not installed on the same machine as modusGate, or if the modusGate machine has more than one NIC, perform the following steps:

WebRoot\Custom.config File

The information contained in this file is required to access the data for WebMonitor.

- If there are multiple NICs on the modusGate server, you may need to replace “localhost” with the first static IP of the server for the following values:
  - Site
  - WebMailServerAddress
  - MonitoringServerAddress
  - Ensure that the Temp and LogDir values point to the correct location for these files
  - If changes are made to the custom.config file, stop and start WEBMAILSVR in the modusGate Console, and IISAdmin on the server

Folder Permissions

Ensure that the appropriate permissions are granted:

Windows 2000 Server

- In Windows Explorer, go to ...\Program Files\Vircom\Web
- Right-click the Web folder and select Properties > Security > Add
- Select IUSR_Machine and ASPNET Accounts
- Click OK
- For the two new Groups/User Names, give Modify permission
- Click on Advanced to replace permission entries on all child objects

Windows Server 2003 and Server 2008

- In Windows Explorer, go to ...\Program Files\Vircom\Web
- Right-click on the Web folder and select Properties > Security
  - Server 2003: click Add
  - Server 2008: click on Edit > Add
- At Select Users or Groups, click on Advanced

- Click on Find Now
  - Select IUSR_Machine and Network Service
  - Click on OK (2x)
- For the two new Groups/User Names, give Modify permission
  - Click on Advanced to replace permission entries on all child objects
  - Click on OK
- Stop/start the IIS service

Performance counters

modusGate supplies a number of Performance Counter objects to help diagnose performance issues, and to help you monitor your system more closely.

To locate the counters, open Windows' Performance Monitor. In the list of Available Counters, you should find each of the following modusGate services (where applicable): Modusadm, Moduscan, Modusmon, SMTPDS, SMTPRS and Webmailsvr. Expand each item to see its list of available counters.

Section 6

Appendices

Appendix A: Web Applications

The following section describes the functions available in the modusGate WebMonitor and WebAdmin applications.

For details about WebQuarantine, see the *WebQuarantine User Guide*, located in the ...Vircom\modusGate\Documents directory.

WebMonitor

The WebMonitor application provides information about system health and the mail statistics. It is preferable to run it on a separate (web) server as it could interfere with modusGate's performance.

An SVG viewer is required to view the interface. Download the SVG viewer from: http://www.abobe.com/svg/viewer/install/

NOTE This application can only be executed in Internet Explorer 6, 7 and 8. IE 9 is not supported.

Login

- WebMonitor uses NT authentication
- Your Windows login ID must have permission to access the folder where WebMonitor is located
  - The default folder is ...\Program Files\Vircom\Web\Webmonitor
- To log into WebMonitor, type /webmonitor/login.aspx after the server URL

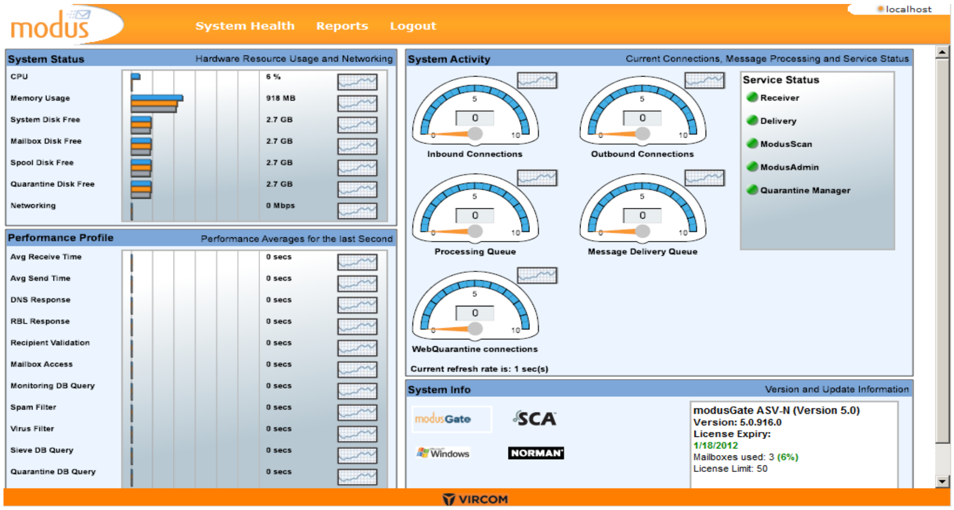
EXAMPLE serveraddress/webmonitor/login.aspx

System Health

The System Health screen provides the following information:

- System Status:
  - Hardware resource usage and networking information
  - Click on a graph icon to see performance trend graphs for the last hour, the last 24 hours and the last week

- System Activity:
  - Inbound and Outbound connections
  - Processing and Message Delivery queues
  - WebQuarantine connections (if installed on a separate server, this will not be available)
- Performance Profile:
  - Average performance rates for messages processed in the last second
- System Info:
  - Version and update information for all systems
- Service Status:
  - Indicates the status of the various services



System Status	Hardware Resource Usage and Networking
CPU	6 %
Memory Usage	918 MB
System Disk Free	2.7 GB
Mailbox Disk Free	2.7 GB
Spool Disk Free	2.7 GB
Quarantine Disk Free	2.7 GB
Networking	0 Mbps

Performance Profile	Performance Averages for the last Second
Avg Receive Time	0 secs
Avg Send Time	0 secs
DNS Response	0 secs
RBL Response	0 secs
Recipient Validation	0 secs
Mailbox Access	0 secs
Monitoring DB Query	0 secs
Spam Filter	0 secs
Virus Filter	0 secs
Sieve DB Query	0 secs
Quarantine DB Query	0 secs

System Activity — Current Connections, Message Processing and Service Status

Inbound Connections: 0
Outbound Connections: 0
Processing Queue: 0
Message Delivery Queue: 0
WebQuarantine connections: 0

Service Status
● Receiver
● Delivery
● ModusScan
● ModusAdmin
● Quarantine Manager

Current refresh rate is: 1 sec(s)

System Info — Version and Update Information

modusGate ASV-N (Version 5.0)
Version: 5.0.916.0
License Expiry:
1/18/2012
Mailboxes used: 3 (6%)
License Limit: 50

Trend Graph Display

There are 3 graphs depicting trends:

- Last hour: average readings at 20 second intervals
- Last 24hrs: average readings at 8 minute intervals
- Last week: average readings at hourly intervals

Activity Gauges

The activity gauges provide a reading of the number of connections or messages that are being processed and the number of messages in the delivery queue at the time of reading. Since the page refreshes every second, the gauges display the most current system information.

The gauge increments are determined dynamically and always in round numbers, i.e. 10, 100 or 1000 depending on the amount of traffic on the system

- The lower threshold is rounded down to the lowest number of activity experienced by the system in the last 24 hours
- The highest threshold will be rounded up to the highest number of activity experienced in the last 24 hours
- Example:
  - If, in the past 24 hours, the lowest number of inbound messages is 9 and the highest is 367, then the Inbound Connections activity gauge increments are between 0 and 400
  - An arrow that is left of center indicates a lower than average load and an arrow that is right of center indicates a higher than average load for the past 24 hours

Service Status

The following identifies the service status colors:

Green – the service is functional

Orange – the service is in the process of starting or stopping

Red – the service is stopped

A service may stop and start on its own because of updates. In Windows, go to Administrative Tools > Services to verify the status of the service.

Performance Profile

modusGate measures average component performance for the delivery/ processing time of messages passing through the system in the last second. If no messages were processed in the last second, the values will be zero (0).

System Info

The System Info panel provides version and update information for the various system components. Click on a logo for information about each individual component:

- modusGate: version, license expiry, number of mailboxes, license limit
- Windows Server: version, last reboot
- SCA: spam engine version and last update
- Norman/McAfee (where applicable): version and last virus engine update

Reporting

This feature allows administrators to schedule and view system, domain, and user-level statistical data. The reports can be printed, exported to PDF and Excel formats and emailed.

With the exception of the System Overview panel, statistical data presented is for the previous day. However, statistics can be shown for a particular day, week, month or year. The date and time of report generation is displayed with the report title.

System Overview

The System Overview provides a snapshot of the system activity for the previous day, the previous week and the previous month.

Mail Traffic Spotlight: displays the previous day's most active sender and recipient of legitimate messages, spam and viruses.

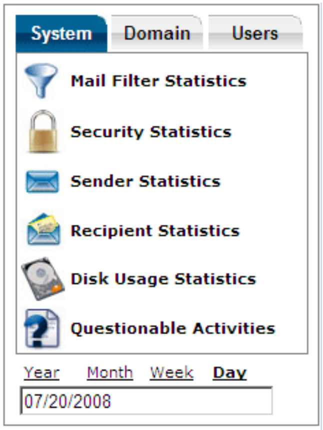
Trend Watch: presents a statistical comparison for the past day, week and month for the following measures:

- Mail Traffic Overview
  - Provides information for the total messages scanned with a percentage breakdown for legitimate and blocked messages
- Blocked Content Breakdown
  - Provides blocked content information, in percentages, for messages blocked by each filter

- Security Overview
  - Provides the number of total connections received by modusGate with a percentage breakdown for connections accepted and connections blocked by all security measures

System

This section provides the following statistical information for the modusGate system.



07/20/2008

Mail Filter Statistics

- Provides a graphical analysis of the messages processed by the system in terms of legitimate mail vs. threats, with a further breakdown of the threat types.
- If any of the filters are disabled, the name will appear in the legend but the value will show N/A. If the function is active but there are no results, the value will be 0.

Security Statistics

- Displays the number of connections blocked per security measure enabled in the Console, and the top 10 RBL servers used, to compare their efficacy.

Sender Statistics

- Identifies the top 10 email message senders (local and external).

Recipient Statistics

- Identifies the top 10 local email message recipients.

Disk Usage Statistics

- Displays the top ten local email addresses that use the most disk storage space, for quarantine and mailbox storage.
- Disk usage statistics are compiled daily at 2:00 AM. As such, the reported values may not reflect the actual values at the time the report is requested. Compilation occurs at this time so as not to interfere with other automated processes and because there is likely to be less mail traffic. This ensures that the system has sufficient time to count all messages on the server.
- It could take several hours to compile the Disk Usage statistics so be aware of this when scheduling the Disk Usage report.

Questionable Activities

Provides information about questionable email activities and can help identify potential abuse:

Highest Volume Senders (Local)

- Lists the top ten email senders (by email address) for all domains on modusGate™
- The Unique Address Count measures the number of recipients per message
  - If a message is sent to a mailing list, the list is expanded to count the number of recipients and only applies to legitimate mail and spam that is tagged and passed
- Messages that are quarantined or deleted for spam, F.A. or virus content are counted as one recipient
- It also can be used to help recognize spamming activity
  - I.e. if one message is sent to 1,000 recipients, it is likely spam

Login Authentication Failures by IP (Including Web Logins)

- Lists the top ten failed authentication logins, both internal and external, by IP address
- Includes the authentication type, the number of rejections and the failure rate
- This feature can help to determine if there were attempts to hack into modusGate

Login Authentication Failures by Email Address (Including Web Logins)

- Lists the top ten failed authentication logins, both internal and external, by email address (i.e. who has attempted to log in)
- Includes the authentication type, the number of rejections and the failure rate
- This feature can help identify if local users are experiencing login problems or determine if there were attacks on modusGate

Domain

This section provides statistical information for individual domains on modusGate. Administrators can retrieve the Mail Filter and Disk Usage statistics by entering the domain name in the Domain field. There is an auto-complete mechanism in place for this.

Users

Provides statistical information for individual users. Administrators can retrieve the Mail Filter statistics by entering the complete email address in the Email field.

Using the calendar

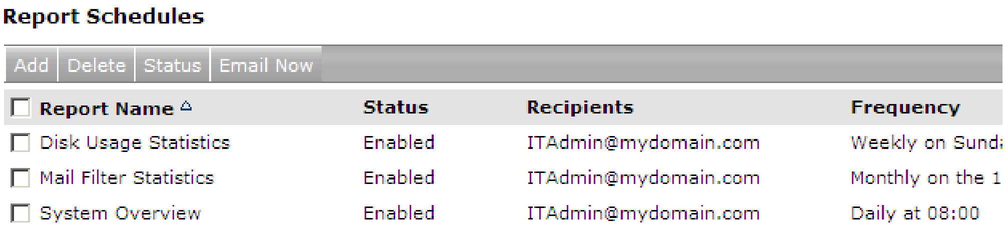
Click on Year, Month, Week or Day to open the particular calendar and make your selection for each of the measures listed above.

Printing and Exporting Reports

All reports can be printed and exported to PDF and Excel.

Report Schedules

Administrators can schedule modusGate to email system reports to the addresses of their choice. All system reports can be delivered in both Excel and PDF formats, and on a daily, weekly or monthly basis. Additionally, administrators can use the Email Now feature to generate an immediate email message for the scheduled report(s).



☐ Report Name	Status	Recipients	Frequency
☐ Disk Usage Statistics	Enabled	ITAdmin@mydomain.com	Weekly on Sund
☐ Mail Filter Statistics	Enabled	ITAdmin@mydomain.com	Monthly on the 1
☐ System Overview	Enabled	ITAdmin@mydomain.com	Daily at 08:00

NOTE When accessing the Report Scheduler for the first time, the error "The system cannot connect with WebMonitor" may appear, along with the System Configuration panel. Copy the URL address from the Address field of the Web browser and paste it into the WebMonitor URL field in the System Configuration. Click on Save.

To schedule a report:

- Select the report type and name
- Set the frequency (can be monthly, weekly or daily)
- Choose the report format (PDF or Excel)
- Enter an address to be displayed in the Email From field; by default the local postmaster address is used (if configured)
- Enter the recipient email address in the Email To field
- To disable/enable scheduled reports, click Status

Message Audit

System administrators can audit email messages to get an up-to-date view of mail processing. Transactions are displayed in a 1-line summary to provide traceability of who sent the message and when, to whom, whether the message was filtered or delivered, and whether the user opened it.

Searching Messages

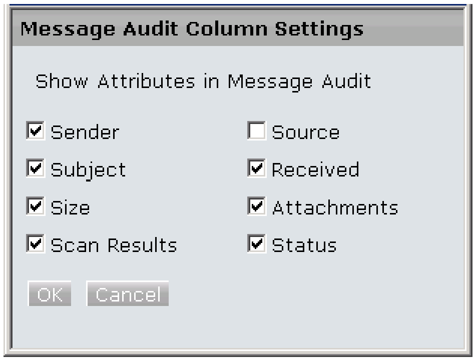
The search feature allows you to search for specific messages in the message audit log using various search criteria, including: date sent, sender/recipient address, subject content, scan results, message status, etc.

Note that, because of database constraints, the default maximum number of results is 100. This setting limits all searches. It can be changed when performing searches, but be aware that the higher the number, the longer the search will take to execute.

Search Results

The search results view can be configured to provide up to eight columns of information

- Click on Settings to select which attributes to present in the search results

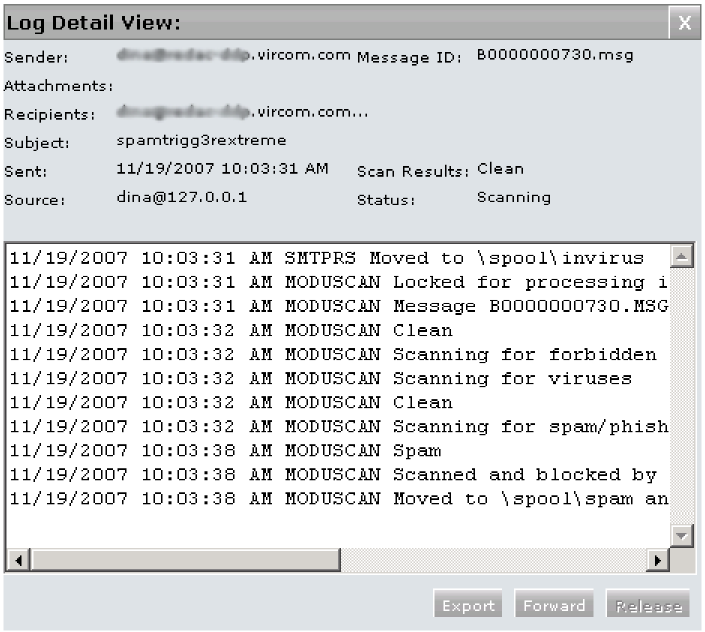


Message Audit Column Settings

Show Attributes in Message Audit

☑ Sender ☐ Source
☑ Subject ☑ Received
☑ Size ☑ Attachments
☑ Scan Results ☑ Status

- To view the Message Audit Log details, click on a particular entry to open the detailed view
  - In addition to the information available in the search results view, the log detail view provides the full transaction history for a particular message



Log Detail View:

Sender: [redacted].vircom.com Message ID: B0000000730.msg
Attachments:
Recipients: [redacted].vircom.com...
Subject: spamtrigg3rextreme
Sent: 11/19/2007 10:03:31 AM Scan Results: Clean
Source: dina@127.0.0.1 Status: Scanning

```
11/19/2007 10:03:31 AM SMTPRS Moved to \spool\invirus
11/19/2007 10:03:31 AM MODUSCAN Locked for processing i
11/19/2007 10:03:31 AM MODUSCAN Message B0000000730.MSG
11/19/2007 10:03:32 AM MODUSCAN Clean
11/19/2007 10:03:32 AM MODUSCAN Scanning for forbidden
11/19/2007 10:03:32 AM MODUSCAN Scanning for viruses
11/19/2007 10:03:32 AM MODUSCAN Clean
11/19/2007 10:03:32 AM MODUSCAN Scanning for spam/phish
11/19/2007 10:03:38 AM MODUSCAN Spam
11/19/2007 10:03:38 AM MODUSCAN Scanned and blocked by
11/19/2007 10:03:38 AM MODUSCAN Moved to \spool\spam an
```

- Click on Export to export the log detail for a particular message to a HTML or text file
- The file can be opened in a Web browser or saved to any location
- Click on Forward to forward the log
  - The message is sent from the postmaster account
- Click on Release to release blocked messages to their destined recipients

WebAdmin

The WebAdmin application provides Web access to the administrative functions of modusGate. Mirroring the Domain and User properties of the Administrative Console, IT administrators can use it to manage modusGate remotely or grant access to domain administrators to manage their own user settings. This can be useful for organizations that host multiple domains.

NOTE Note that the WebAdmin feature is not available for unlimited user licenses. In addition, because the functions in WebAdmin are identical to those in the Console, the information contained in this section is limited. Complete details can be found throughout this guide.

Login

To log into WebAdmin, type /webadmin after the server URL

EXAMPLE E.g. serveraddress/webadmin

It may take several seconds to log into WebAdmin for large deployments because of the message statistics view. If faster access is required, the statistics view can be disabled:

1. With Notepad, open the Web.config file located in ...\Vircom\Web\WebAdmin\Root

2. Locate <add key="ShowStats" value="true"/>

3. Replace “true” with “false”

4. Save the file.

WebAdmin was developed for system and domain administrators. Access should not be given to end users. The Log in as user feature was designed for use by administrators to verify changes made for a specific user.

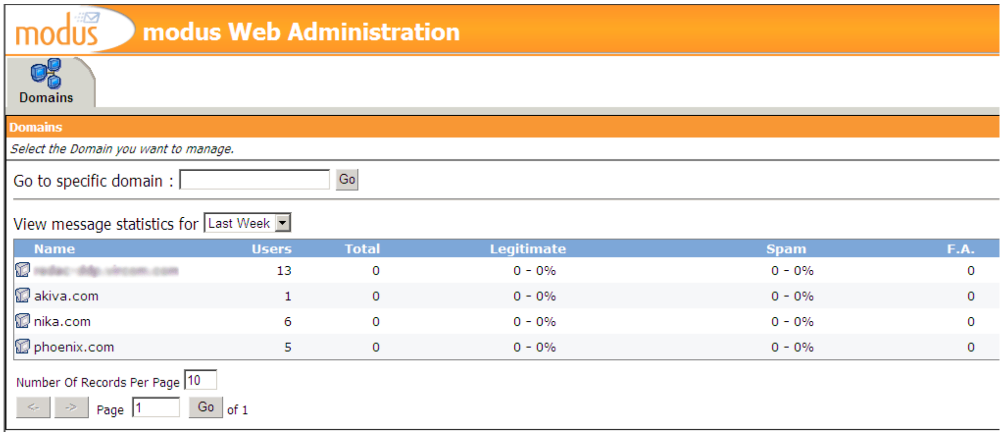
Before users can access WebAdmin, they must be granted permission. For details, see *"WebAdmin Privileges" on page 107*.

Domains

The main panel provides access to the configuration options as well as providing a summary of the message statistics for your domain(s) and users.

Statistics are available for the Last Day, Last Week and Last Month. Use the drop-down menu to select the time period.

Click Edit to access the specific domain or enter a domain name and click Go.



Domains

Select the Domain you want to manage.

Go to specific domain : ______ Go

View message statistics for Last Week

Name	Users	Total	Legitimate	Spam	F.A.
[redacted]	13	0	0 - 0%	0 - 0%	0
akiva.com	1	0	0 - 0%	0 - 0%	0
nika.com	6	0	0 - 0%	0 - 0%	0
phoenix.com	5	0	0 - 0%	0 - 0%	0

Number Of Records Per Page 10

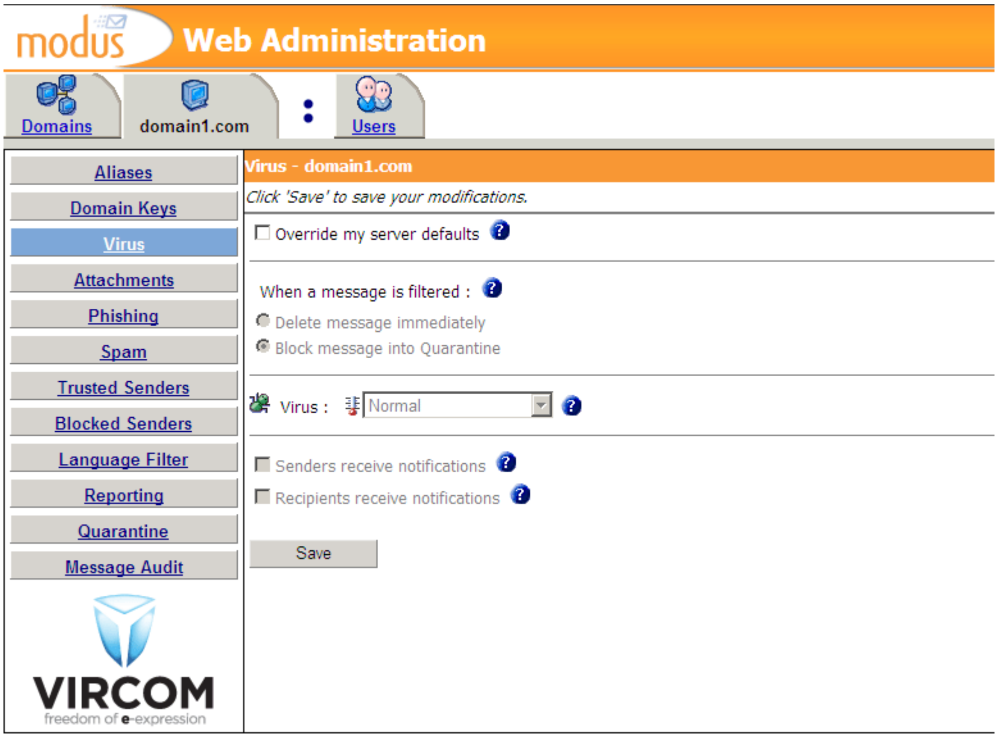
<- -> Page 1 Go of 1

Domain View

The Domain panel provides access to the following configuration panels. All settings available in the Console are also available here:

- Aliases: manage aliases for the domain
- Domain Keys: View the domain key and enable DKIM for outbound messages
- Virus: override the system defaults for virus handling
- Attachments: override the system defaults for processing messages containing forbidden attachments
- Phishing: override the system defaults for processing phishing messages
- Spam: override the system defaults for processing spam messages

- Trusted Senders: manage the trusted senders list for the domain
- Blocked Senders: manage the blocked senders list for the domain
- Language Filters: override the system defaults for processing messages with foreign language content and configuring blocked languages
- Reporting: override the system defaults for the Quarantine Report frequency, content and settings
- Quarantine: manage (delete and release) quarantined mail by category: spam, attachments, phishing and viruses
- Message Audit: override the system defaults for message audit logging



Virus - domain1.com

Click 'Save' to save your modifications.

□ Override my server defaults

When a message is filtered :

○ Delete message immediately

● Block message into Quarantine

Virus : Normal

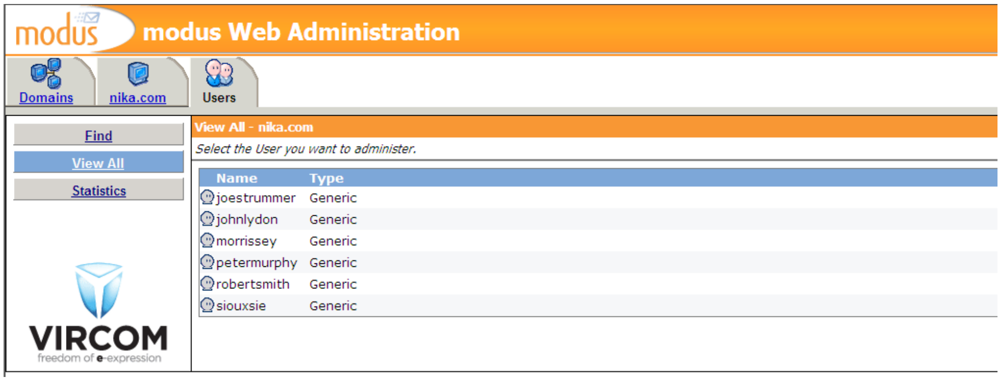
□ Senders receive notifications

□ Recipients receive notifications

Users

From the Users panel, you have access to the following configuration panels:

- Find: search for a specific user
- View All: view all users for the specific domain and access the configuration panel for it
- Statistics: view message statistics for each user on the domain



View All - nika.com

Select the User you want to administer.

Name	Type
joestrummer	Generic
johnlydon	Generic
morrissey	Generic
petermurphy	Generic
robertsmith	Generic
siouxsie	Generic

User View

From the Users panel, you have access to the following configuration panels. All settings available in the Console are also available here.

- Virus: specify how modusGate should process messages that contain viruses
- Attachments: specify how modusGate should process messages that contain forbidden attachments
- Phishing: specify how modusGate should process phishing messages
- Spam: specify how modusGate should process spam messages and configure the spam filter by category
- Reporting: configure the user’s Quarantine Report frequency and content
- Trusted Senders: manage trusted senders for the user
- Blocked Senders: manage blocked senders for the user
- Language Filter: specify how modusGate should process messages with foreign language content and configure blocked languages
- Aliases: manage aliases for the user
- Quarantine: manage (delete and release) the user’s quarantined mail by category: spam, attachments, phishing and viruses
- Message Audit: manage the user’s message audit settings

Appendix B: Formal Command Syntax

The SMTPDS and SMTPRS services may be controlled from a command line by using command-line arguments.

The following options apply for both SMTPRS and SMTPDS.

Syntax

```
smtprs [-remove | -install] [-version]
   [-ipaddress] [-status] [-start]
   [-stop]
```

Options

- -install: adds the SMTPRS server to the list of installed services
- -remove: removes the SMTPRS server from the list of installed services, and will delete the SMTPRS server-specific configuration information from the Registry
- -version: reports the version number of SMTPRS server
- -ipaddress: reports the IP address(es) used for SMTPRS connections
- -status: reports the current status of the SMTPRS server, i.e. whether or not it is running
- -start: starts the SMTPRS server
- -stop: stops the SMTPRS server

Appendix C: Interacting with Exchange

This section explains how modusGate interacts with Exchange and Active Directory.

Disabled user objects:

- When an account is disabled in Active Directory, it can no longer access the server to use server and network resources.
- Mailbox attributes assigned to the disabled account may be kept.
- When modusGate performs a lookup on an AD object, it does not check the status of the account (enabled or disabled).
  - It looks for specific flags to determine if the user's mailbox is enabled.
  - This ensures that, if Exchange is routing mail for the object, modusGate creates an account for the object and route mail to the Exchange server for processing.

Secure LDAP with AD:

- When modusGate performs LDAP authentication over a SSL secured link with a Domain Controller, AD only accepts User DN values in the form of username@domain.local.
  - When modusGate searches for account information while performing user authentication, it uses the user principal name as the default authentication account.
- If the user principal name is not used, you will need to fill in this account.

Forwarded accounts

- When an email enabled account in Active Directory specifies an external email domain in its primary SMTP address attribute, Exchange re-routes the message to the user's specified external account

- Example:
  - Local domain = mymaildomain.com
  - Domain configured in modusGate = mymaildomain.com
  - Local user’s primary email attribute = user1@mymaildomain.com
  - External user’s primary email attribute value = user2@hismaildomain.com
  - External user’s secondary email attribute value = user2@mymaildomain.com
  - If mail is sent to user1, the message is processed normally and delivered to user1’s mailbox
  - If mail is sent to user2, the external account is added as an alias to the account hosted in modusGate™ so that mail is delivered to user2’s mailbox
  - Users with external accounts cannot log into WebQuarantine with their alias addresses
  - They can only log into WebQuarantine with an account entered in the users directory

Appendix D: Trusted and Blocked Senders Behaviors

This section provides information about the behaviors for the Trusted and Blocked Senders lists, including the way various security checks are processed:

Trusted and Blocked Senders lists can be created at the system, domain and user levels. The following is the sequence of events that occurs once modusGate receives a message:

- Check the connection limits (total connections & maximum connection rate and the total simultaneous connections from the same IP address & simultaneous connection rate from the same IP address)
  - Bypass this test if a host is in the trusted list or in transparent mode (i.e. when modusGate hides a source IP address)
- Check for required authentication
  - If SMTP authentication is enabled and is forced and the host is in the list of forced authentication IP addresses, authentication is required (Security > SMTP Security)
- Reject all connections from hosts in the Reject all incoming mail from list (Security > Connections)
- Simultaneously start reverse and RBL lookups if the following conditions are met:
  - Reverse DNS or RBL lookup or both are enabled (Security > Sender Reputation and Real-Time Blacklist)
  - The host is not in the trusted list
  - RBL lookup is enabled and the host is not in the IP address exclusion list for RBL lookups
  - The connection does not come from one of the routed IP addresses in modusGate, and modusGate is configured to hide a protected server (i.e. placed in front of the mail server)
- Place the RBL lookup result in the envelope of the received message
- If reverse DNS is enabled and fails, the connection is refused with the default message "This system is configured to reject mail from host [*IP address*]. DNS reverse lookup failed."
- If the host is found on an RBL, the envelope will contain the header *X-Modus-RBL will be set to IP= Blacklisted*. Furthermore, if Reject connection immediately if the host is blacklisted is enabled (Security > Real-Time Blacklist) and Postpone the rejection until authentication is disabled (Security > Sender Reputation), the connection will be rejected.
- If the host is found on an RBL and Postpone the rejection until authentication is enabled, the decision will be delayed until the user can be authenticated

- At the Mail From: command, if reverse DNS is enabled and fails, or if RBL lookup is enabled and fails and modusGate is not configured to reject the connection immediately if the host is blacklisted, the connection is rejected

- After the Mail From: command, modusGate checks for SPF support and performs a Look up for SMTP host in the real-time whitelist servers, if enabled (Security > Sender Reputation)

- At the scanning stage, modusGate does not scan internally-generated messages or messages from IP addresses in the list of trusted addresses (Security > Trusted Address List > Scanning Trusted Address)

- If the message contains an attachment greater than the configured limit, modusGate does not scan it (Rules > Performance > Attachment Size Verification)

- modusGate does not scan messages from SMTP authenticated users (this is configurable) but it always scans for forbidden attachments and viruses

- Checks the scan properties for each recipient (e.g. spam, virus & attachment scanning levels)

- Checks the Trusted and Blocked Senders lists for each recipient

Section 7

Glossary

Glossary

Address / Email Harvesting

The process of obtaining lists of email addresses for use in bulk mail or spam.

Alias

An alias is an email address that forwards all email it receives to another email account.

Catch Rate

The catch-rate measures the efficiency of a spam solution. The calculation used is: (# of spam messages caught   # of total spam messages) x 100

Content Filtering

Spam scanning plain text for key phrases and the percentage of HTML, images and other indications that the message is spam.

Denial of Service (DoS)

An attempt to make a computer resource unavailable to its intended users. Considered an Internet crime.

Dictionary Attack

A system of combining letters and numbers in an attempt to find active email addresses. Any addresses to which messages are delivered, as opposed to being bounced back, are legitimate.

Directory Service

A network service that identifies all resources on a network and makes them accessible to users and applications. The software stores and organizes information about a computer network's users and network shares and allows network administrators to manage users' access to the shares. Resources include email addresses, computers and peripheral devices. There are a number of directory services that are used, including Active Directory and LDAP.

DNSBL

DNS Block List. *See* RBL.

ESMTP

Extended SMTP. *See* SMTP.

False Negative

A false negative occurs when spam is not recognized by a spam solution and delivered to a mail inbox.

False Positive

A false positive occurs when legitimate mail is incorrectly recognized by a spam solution and not delivered to a mail inbox.

Filter Scripting

Advanced filtering logic method to block many or all spam tactics.

Fingerprinting

Smart file type detection. A technology that scans email attachments in search of forbidden file formats (e.g. *.exe) in order to prevent them from concealed with modified file extensions.

Headers

The top portion of a message that contains the sender's name, date the message was sent, recipients' names, title, routing details, message priority, and other information.

LDAP

Lightweight Directory Access Protocol. Standard protocol for the exchange of directory entries between servers.

LDIF

LDAP Data Interchange Format. The format used by an LDAP server when returning information for LDAP requests.

MIB

Management Information Base. A MIB is a file that contains descriptions about the characteristics of a modusGate Server (or any other managed device on a network for which a MIB has been created). The characteristics described in the MIB are the functional elements for the modusGate Server which can be monitored using SNMP software.

NVC

Norman Virus Control. Software sold by Norman Data Defense that provides server-side anti-virus protection. modusGate uses the same virus definition files as Norman Virus Control.

ODBC

Open Database Connectivity. ODBC is an application programming interface (API) used to access third-party databases.

Open Proxy

A proxy that allows computers to use it to make connections to services on their behalf, whether they would normally have permission to access the service or not.

Open Relay

An SMTP (mail) server configured in such a way that it allows anyone on the Internet to relay (i.e. send) mail through it. Often open to attack and hijacked to send large amounts of spam.

Phishing

A scam that uses spam to deceive people into disclosing their credit card numbers, bank account information, passwords and other sensitive information. Phishers often masquerade as trustworthy or well-known businesses.

POP3

Post Office Protocol 3. A standard mail protocol for authenticating and retrieving mail over the Internet. Unlike IMAP (where mail resides on the server), POP3 moves messages from the server to the users' computers.

Quarantine

Mail that has been blocked because of suspicious content, viruses or forbidden attachments.

RBL

Real-time Black List. A DNS-based Blackhole List (DNSBL, also known as Real-time Blackhole List or RBL), is a means by which an Internet site may publish a list of IP addresses, in a format which can be easily queried by computer programs on the Internet A free service offered by some organizations such as ORBS or MAPS that provides a list of known spammers, updated in real-time. This term is used interchangeably with DNSBL

Reverse DNS

A process to determine the hostname associated with a given IP address. This feature ensures that users are from legitimate domains.

Sieve

Simple scripting language used to filter email. One of the more powerful features of sieve is filtering spam. Sieve is defined in RFC3028.

SMTP

Simple Mail Transport Protocol. The protocol used to deliver email to its destination.

SNMP

Simple Network Management Protocol. SNMP is part of the TCP/IP protocol. SNMP applications run in a network management station (NMS) and issue queries to gather information about the status, configuration, and performance of external network devices.

Spam

Unsolicited, bulk email. Also known as junk mail.

SPF

Sender Policy Framework. SPF helps to prevent return-path address forgery and makes it easier to identify spoofs. For more information, go to www.openspf.org or RFC 4408.

Spoof

In the context of network security, a spoofing attack is a situation in which a person or program successfully masquerades as another by falsifying data. With phishing, a legitimate Web page (such as a bank's) is reproduced in *look and feel* by the phisher. The intent is to trick users into thinking that they are connected to a trusted site. The phisher then harvests personal information.

SURBL

Spam URI Real-time Block Lists. A SURBL detects spam messages based on message body URIs instead of the spam senders. They allow you to block messages that have spam hosts mentioned in the message bodies. For more information, go to www.surbl.org.

URI

A string of characters used to identify or name a resource. The main purpose is to enable interaction with representations of the resource over the Internet using specific protocols.

URL

Universal or Uniform Resource Locator. An Internet address used by Web browsers to access a specific site or a document (resource).

Virus

Any piece of code that replicates and executes itself. Viruses usually deliver a piece of malicious code that carries out a destructive operation on the host machine.